GarrettCom
A BELDEN BRAND

MAGNUM 12KX SWITCH

Version 00.7.xx

Administrator Guide

Preface

This guide describes how to use the Magnum 12KX switch.

Some simple guidelines which will be useful for configuring and using the Magnum 12KX switches

- If information on a specific command is needed in the CLI, type the command name after typing the word “help” (help <*command*>) or just type <command> [Enter].
- If information on a specific feature in Web Management Interface is needed, use the online help provided in the interface.
- If further information or data sheets on GarrettCom Magnum 12KX family of switches is needed, refer to the GarrettCom web pages at www.garrettcom.com .

GarrettCom Inc.
47823 Westinghouse Drive
Fremont, CA 94539-7437
Phone (510) 438-9071• Fax (510) 438-9072
Email – Tech support – support@garrettcom.com
Email – Sales – sales@garrettcom.com
WWW – http://www.garrettcom.com/

Trademarks

GarrettCom Inc. reserves the right to change specifications, performance characteristics and/or model offerings without notice. GarrettCom, Magnum, S-Ring, Link-Loss-Learn, Converter Switch, Convenient Switch and Personal Switch are trademarks and Personal Hub is a registered trademark of GarrettCom, Inc.

NEBS is a registered trademark of Telcordia Technologies.

UL is a registered trademark of Underwriters Laboratories.

Ethernet is a trademark of Xerox Corporation.

The naming of copyrighted trademarks in this manual, even when not specially indicated, should not be taken to mean that these names may be considered as free in the sense of the trademark and trade name protection law and hence that they may be freely used by anyone.

GarrettCom reserves the right to change the contents of this document without prior notice. GarrettCom can give no guarantee in respect of the correctness or accuracy of the information in this document.

GarrettCom can accept no responsibility for damages, resulting from the use of the network components or the associated operating software. In addition, we refer to the conditions of use specified in the license contract.

Printed in the United States of America.

Part #: 84-00190Z

PK-102511

Table of Contents

List of Figures

List of Tables

About this Manual

The “Basic Configuration” user manual contains the information needed to start operating the device. It contains step by step information from the first startup operation through to the basic settings for operation in the user environment.

The following thematic sequence has proven itself in practice:

- Set up device access for operation by entering the IP parameters
- Check the status of the software and update it if necessary
- If a configuration already exists, load/store it
- Configure the ports
- Set up protection from unauthorized access
- Optimize the data transmission with network load control
- Synchronize system time in the network
- Function diagnosis
- Store the newly created configuration to nonvolatile memory

The "Command Line Interface" reference manual contains detailed information on using the Command Line Interface to operate the individual functions of the device.

Key

The designations used in this manual have the following meanings:

▶	List
☐	Work step
■	Subheading
Link	Indicates a cross-reference with a stored link
Note:	A note emphasizes an important fact, or draws attention to a dependency.
`Courier`	ASCII representation in user interface

Execution in the Web-based Interface user interface

Execution in the Command Line Interface user interface

Symbols used

	WLAN access point
	Router with firewall
	Switch with firewall
	Router
	Switch
	Bridge
	Hub
	A random computer
	Configuration Computer
	Server

PLC - Programmable logic -controller

I/O - Robot

Introduction

The Magnum 12KX has been developed for practical application in a harsh industrial environment. Accordingly, the installation process has been kept simple. Thanks to the selected default settings, only a few settings need to be entered before starting to operate Magnum 12KX.

Note: The changes made in the dialogs are copied into the volatile memory of the Magnum 12KX when on "Set" is clicked.
To save the changes into the permanent memory of the device select the non-volatile memory location in the `Basic Settings:Load/Save` dialog and click "Save".

Chapter 1

Access to the user interfaces

The device has 3 user interfaces, which can be accessed via different interfaces:

- System monitor via the V.24 interface (out-of-band)
- Command Line Interface (CLI) via the V.24 connection (out-of-band) as well as Telnet or SSH (in-band)
- Web-based interface via Ethernet (in-band).

System Monitor

The system monitor enables user to

- select the software to be loaded
- perform a software update
- start the selected software
- shut down the system monitor
- delete the configuration saved and
- display the boot code information.

Opening the system monitor

☐ Use the terminal cable (see accessories) to connect
– the V.24 socket (RJ11) to
– a terminal or a COM port of a PC with terminal emulation based on VT100
(for the physical connection, see the "Installation" user manual).

Speed	9,600 Baud
Data	8 bit
Parity	none
Stopbit	1 bit
Handshake	off

Table 1: Data transfer parameters.

☐ Start the terminal program on the PC and set up a connection with the Magnum 12KX.

When the Magnum 12KX is booted, the message
"Press <1> to enter System Monitor 1"
appears on the terminal.

```
< Device Name  (Boot) Release: 1.00 Build: 2005-09-17 15:36 >

Press <1> to enter System Monitor 1 ...
 1
```

FIGURE 1 Screen display during the boot process.

- ☐ Press the <1> key within one second to start system monitor 1.

```
   System Monitor

   (Selected OS: L3P-01.0.00-K16 (2005-10-31 19:32))

   1  Select Boot Operating System
   2  Update Operating System
   3  Start Selected Operating System
   4  End (reset and reboot)
   5  Erase main configuration file


sysMon1>
```

FIGURE 2 – System monitor 1 screen display

- ☐ Select a menu item by entering the number.
- ☐ To leave a submenu and return to the main menu of system monitor 1, press the <ESC> key.

Command Line Interface

The Command Line Interface enables the user to use the functions of the Magnum 12KX via a local or remote connection. The Command Line Interface provides IT specialists with a familiar environment for configuring IT devices.

The script compatibility of the Command Line Interface enables the user, among other things, to feed multiple devices with the same configuration data, to create and apply partial configurations or to compare 2 configuration by comparing the script files.

A detailed description of the Command Line Interface can be found in the "Command Line Interface" reference manual.

The Command Line Interface can be accessed via

- the V.24 port (out-of-band)
- Telnet (in-band)
- SSH (in-band)

Note: To facilitate making entries, CLI provides the option of abbreviating keywords. Type in the beginning of a keyword. When the tab key is pressed, CLI completes the keyword.

Opening the Command Line Interface

☐ Connect the Magnum 12KX to a terminal or to the COM port of a PC using terminal emulation based on VT100 and press any key or
call up the Command Line Interface via Telnet.
A window for entering the user name appears on the screen.
Up to five users can access the Command Line Interface.

```
This system is for the use of authorized users only.
Individuals using this system are subject to having their activities
monitored and recorded by authorized company personnel.
Anyone using this system expressly consents to such monitoring and is
advised that if such monitoring reveals possible evidence of criminal
activity, company personnel may provide the evidence of such monitoring
to enforcement officials.

                    Copyright (c) 2011 GarrettCom

                         All rights reserved

      GarrettCom Magnum 12KX Managed L3 Switch Release L3-07.0.03-B31G

                    (Build date 2011-10-12 12:46)


                   System Name:  Magnum 12KX
                   Mgmt-IP    :  192.168.15.110
                   1.Router-IP:  0.0.0.0
                   Base-MAC   :  00:80:63:D7:F3:00
                   System Time:  2011-10-23 19:39:19


(Magnum 12KX)
```

FIGURE 3 – Logging in to the Command Line Interface program.

☐ Enter a user name. The default setting for the user name is **manager** with a password of **manager** . Press the Enter key.

☐ Alternately, the user can login with the login name of **operator** with a password of **operator**. The operator userid does not have administrative privileges.

The user name and the password can be changed later in the Command Line Interface.
Please note that these entries are case-sensitive.

The start screen appears.

```
NOTE: Enter '?' for Command Help. Command help displays all options
      that are valid for the 'normal' and 'no' command forms.  For
      the syntax of a particular command form, please consult the
      documentation.


(Magnum 12KX) >
```

FIGURE 4 – CLI screen after login.

Web-based Interface

The user-friendly Web-based interface gives the option of operating the Magnum 12KX from any location in the network via a standard browser such as Mozilla Firefox or Microsoft Internet Explorer.
As a universal access tool, the Web browser uses an applet which communicates with the Magnum 12KX via the Simple Network Management Protocol (-SNMP).
The Web-based interface allows the user to graphically configure the Magnum 12KX.

Opening the Web-based Interface

To open the Web-based interface, a Web browser is needed (a program that can read hypertext), for example Mozilla Firefox version 7 or later, or Microsoft Internet Explorer version 6 or later.

Note: The Web-based interface uses Java software 6 (“Java™ Run-time Environment Version 1.6.x”).

☐ Start Web browser.
☐ Check that JavaScript and Java have been activated in the browser settings.
☐ Establish the connection by entering the IP address of the device which needs to be administered via the Web-based management in the address field of the Web browser. Enter the address in the following form:
`http://xxx.xxx.xxx.xxx`

The login window appears on the screen.

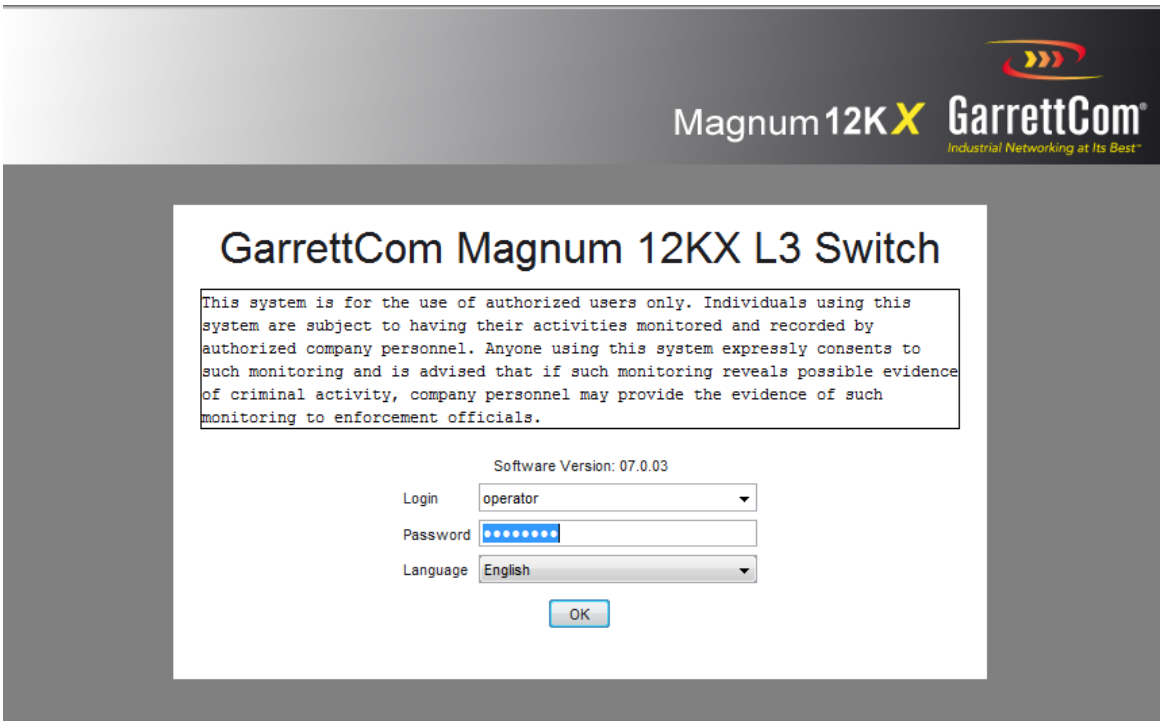


FIGURE 5 – Login window.

☐ Select the desired language.
☐ In the drop-down menu, select
– user, to have read access, or
– admin, to have read and write access
to the Magnum 12KX.
☐ The password "public", with which the user has read access, appears in the password field. If write access is available to the Magnum 12KX, then highlight the contents of the password field and overwrite it with the password "private" (default setting).
☐ Click on OK.

The website of the Magnum 12KX appears on the screen.

Note: The changes made in the dialogs are copied to the Magnum 12KX when "Set" is selected. Click "Reload" to update the display.

Note: The Administrator can block access to the Magnum 12KX by entering an incorrect configuration. Activating the function "Cancel configuration change" in the "Load/Save" dialog enables the user to return automatically to the last configuration after a set time period has elapsed. This returns access to the Magnum 12KX.

Chapter 2

IP Address for the Switch

The IP parameters must be entered when the Magnum 12KX is used for the first time.

The Magnum 12KX provides seven different options for entering the IP parameters during the first installation:

- Entry using the Command Line Interface (CLI).
  Choose this “out of band” method if
  - the user pre-configures the Magnum 12KX outside its operating environment
  - the user does not have network access (“in-band”) to the Magnum 12KX
- Entry using the HiDiscovery protocol using HiVision software.
  Choose this “in-band” method if the Magnum 12KX is already installed in the network or if there is another Ethernet connection between the PC and the Magnum 12KX
- Configuration using the Auto-Configuration Adapter (ACA).
  Choose this method if the Magnum 12KX is being replaced with a device of the same type and have already saved the configuration on an ACA.
- Using BOOTP.
  Choose this “in-band” method if the installed Magnum 12KX needs to be configured using BOOTP. A BOOTP server is needed for this. The BOOTP server assigns the configuration data to the Magnum 12KX using its MAC address. Because the Magnum 12KX is delivered with “DHCP mode” as the entry for the configuration data reference, this has to be reset to the BOOTP mode for this method.
- Configuration via DHCP.
  Choose this “in-band” method if the installed Magnum 12KX needs to be configured using DHCP. A DHCP server is needed for this. The DHCP server assigns the configuration data to the Magnum 12KX using its MAC -address or its system name.
- Using DHCP Option 82.
  Choose this “in-band” method if the installed Magnum 12KX needs to be configured using DHCP Option 82. A DHCP server with Option 82 is needed for this. The DHCP server assigns the configuration data to the Magnum 12KX using its physical connection.
- Configuration via the Web-based interface.
  If the Magnum 12KX already has an IP address and can be reached via the network, then the Web-based interface provides the user with another option for configuring the IP parameters.

IP Parameter Basics

IP address (version 4)

The IP addresses consist of 4 bytes. These 4 bytes are written in decimal notation, separated by a decimal point.

Since 1992, five classes of IP address have been defined in the RFC-1340.

Class	Network address	Host address	Address range
A	1 byte	3 bytes	1.0.0.0 to 126.255.255.255
B	2 bytes	2 bytes	128.0.0.0 to 191.255.255.255
C	3 bytes	1 byte	192.0.0.0 to 223.255.255.255
D			224.0.0.0 to 239.255.255.255
E			240.0.0.0 to 255.255.255.255

Table 2: IP Address Classes.

The network address is the fixed part of the IP address. The worldwide leading regulatory board for assigning network addresses is the IANA (Internet Assigned Numbers Authority). If the user requires an IP address block, contact the Internet service provider. Internet service providers should contact their local higher-level organization:

- APNIC (Asia Pacific Network Information Center) - Asia/Pacific Region
- ARIN (American Registry for Internet Numbers) - Americas and Sub--Sahara Africa
- LACNIC (Regional Latin-American and Caribbean IP Address Registry) – Latin America and some Caribbean Islands
- RIPE NCC (Réseaux IP Européens) - Europe and Surrounding Regions

An IP address belongs to class A if its first bit is a zero, i.e. the first decimal number is less than 128. The IP address belongs to class B if the first bit is a one and the second bit is a zero, i.e. the first decimal number is between 128 and 191. The IP address belongs to class C if the first two bits are a one, i.e. the first decimal number is higher than 191.

Assigning the host address (host id) is the responsibility of the network operator. He alone is responsible for the uniqueness of the IP addresses he assigns.

Netmask

Routers and gateways subdivide large networks into subnetworks. The netmask assigns the IP addresses of the individual devices to a particular subnetwork.

The division into subnetworks with the aid of the netmask is performed in much the same way as the division of the network addresses (net id) into classes A to C.

The bits of the host address (host id) that represent the mask are set to one. The remaining bits of the host address in the netmask are set to zero (see the following examples).

Example of how the network mask is used

In a large network it is possible that gateways and routers separate the management agent from its management station. How does addressing work in such a case?

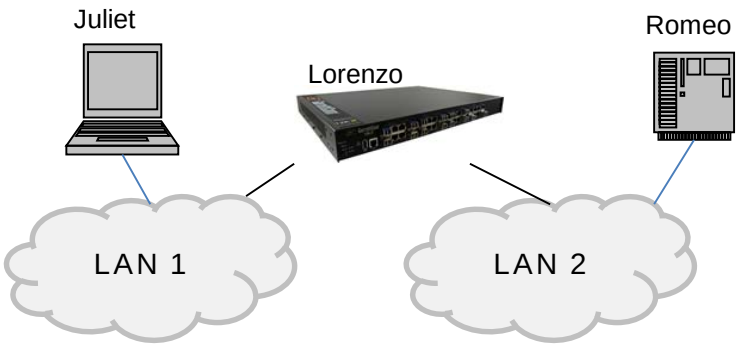


FIGURE 6 – Management agent that is separated from its management station by a router.

The management station "Romeo" wants to send data to the management agent "Juliet". Romeo knows Juliet's IP address and also knows that the router "Lorenzo" knows the way to Juliet.

Romeo therefore puts his message in an envelope and writes Juliet's IP address as the destination address. For the source address he writes his own IP address on the envelope.

Romeo then places this envelope in a second one with Lorenzo's MAC address as the destination and his own MAC address as the source. This process is comparable to going from layer 3 to layer 2 of the ISO/OSI base reference model.

Finally, Romeo puts the entire data packet into the mailbox. This is comparable to going from layer 2 to layer 1, i.e. to sending the data packet over the Ethernet.

Lorenzo receives the letter and removes the outer envelope. From the inner envelope he recognizes that the letter is meant for Juliet. He places the inner envelope in a new outer envelope and searches his address list (the ARP table) for Juliet's MAC address. He writes her MAC address on the outer envelope as the destination address and his own MAC address as the source address. He then places the entire data packet in the mail box.

Juliet receives the letter and removes the outer envelope. She finds the inner envelope with Romeo's IP address. Opening the inner envelope and reading its contents corresponds to transferring the message to the higher protocol layers of the SO/OSI layer model.

Juliet would now like to send a reply to Romeo. She places her reply in an envelope with Romeo's IP address as destination and her own IP address as source. But where is she to send the answer? For she did not receive Romeo's MAC address. It was lost when Lorenzo replaced the outer envelope.

In the MIB, Juliet finds Lorenzo listed under the variable NetGatewayIPAddr as a means of communicating with Romeo. She therefore puts the envelope with the IP addresses in a further envelope with Lorenzo's MAC destination address.

The letter now travels back to Romeo via Lorenzo, the same way the first letter traveled from Romeo to Juliet.

Classless Inter-Domain Routing

Class C with a maximum of 254 addresses was too small, and class B with a maximum of 65534 addresses was too large for most users, as they would never require so many addresses. This resulted in ineffective usage of the Class B addresses available.

Class D contains reserved multicast addresses. Class E is reserved for experimental purposes. A gateway not participating in these experiments ignores datagrams with these destination addresses.

Since 1993, RFC-1519 has been using Classless Inter Domain Routing (CIDR) to provide a solution to get around these problems. CIDR overcomes these class boundaries and supports classless address ranges.

With CIDR, enter the number of bits that designate the IP address range. Represent the IP address range in binary form and count the mask bits that designate the netmask. The netmask indicates the number of bits that are identical to the network part for all IP addresses in a given address range. Example:

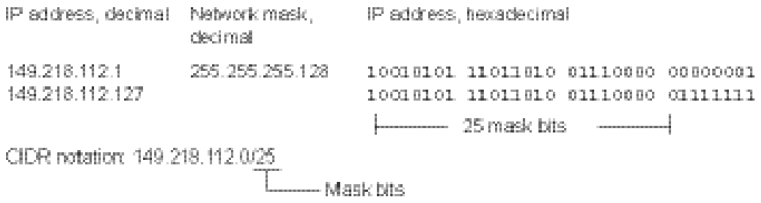


FIGURE 7 – Example of CIDR

The combination of a number of class C address ranges is known as “supernetting”. This enables the user to subdivide class B address ranges to a very fine degree.

Entering IP parameters via CLI

If the IP parameters for the system are not setup via BOOTP/DHCP, DHCP Option 82, the HiDiscovery protocol or the Auto-Configuration Adapter ACA, then the configuration needs to be set via the V.24 interface using the CLI.

Note: If there is no terminal or PC with terminal emulation available in the vicinity of the installation location, the user can configure the Magnum 12KX at their own workstation by taking it to its final installation location.

☐ Set up a connection to the Magnum 12KX via a console (V.24) cable as described earlier.

The start screen appears.

```
NOTE: Enter '?' for Command Help. Command help displays all options
      that are valid for the 'normal' and 'no' command forms.  For
      the syntax of a particular command form, please consult the
      documentation.


(Magnum 12KX) >
```

FIGURE 8 – Welcome screen after a successful login

☐ Deactivate DHCP.

☐ Enter the IP parameters.

- Local IP address
  By default setting is 0.0.0.0.
- Netmask
  If the network has been divided up into subnetworks, and if these are identified with a netmask, then the netmask is to be entered here.
  The default setting of the netmask is 0.0.0.0.
- IP address of the gateway
  This entry is only required if the Magnum 12KX and the management station or tftp server are located in different subnetworks.
  Enter the IP address of the gateway between the subnetwork with the Magnum 12KX and the path to the management station.
  The default setting of the IP address is 0.0.0.0.

☐ Save the configuration entered using

```
copy system:running-config nvram:startup-config.
```

FIGURE 9 – Saving the system configuration using the CLI

`enable`	**Switch to the Privileged EXEC mode.**
`network protocol none`	**Deactivate DHCP.**
`network parms 10.0.1.23 255.255.255.0`	**Assign the** Magnum 12KX **the IP address 10.0.1.23 and the netmask 255.255.255.0. The user has the option of also assigning a gateway address.**
`copy system:running-config nvram:startup-config`	**Save the current configuration to the non-volatile memory.**

FIGURE 10 – Sequence of steps needed to configure the system IP address using CLI

After entering the IP parameters, the Magnum 12KX can be easily cofigured via the Web--based interface (see the “Web-based Interface” reference manual).

Entering the IP Parameters via HiDiscovery

The HiDiscovery protocol enables the user to assign IP parameters to the Magnum 12KX via the Ethernet. The user can easily configure other parameters via the Web--based interface (see the "Web-based Interface" reference manual).

Install the HiDiscovery software on the user PC. The software is available from Hirschmann, a subsidiary of Belden Inc.

Note: The installation of HiDiscovery includes the installation of the software package WinPcap Version 3.1.

If an earlier version of WinPcap is on the PC, the follow the suggestion in the set-up to uninstall it.
A newer version remains intact during the installationHiDiscovery. However, this cannot be guaranteed for all future versions of WinPcap. In the event that the installation of HiDiscovery has overwritten a newer version of WinPcap, uninstall WinPcap 3.1 and then re-install the new version.

☐ Start the HiDiscovery program.

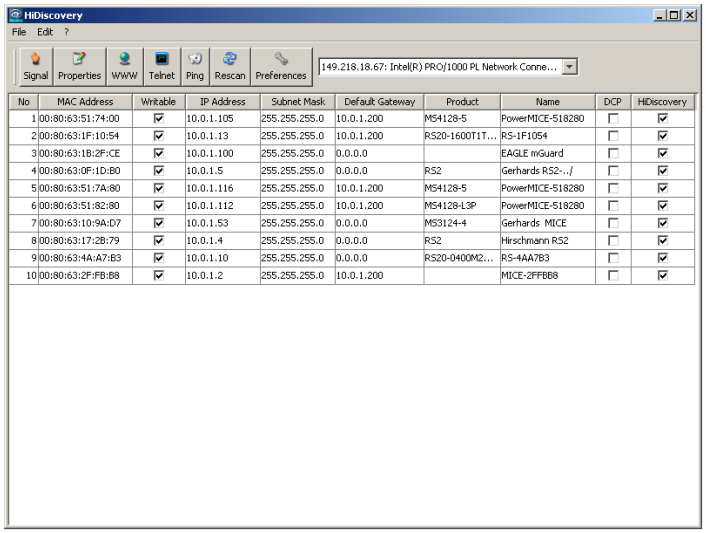


FIGURE 11 – HiDiscovery displaying different devices discovered

When HiDiscovery is started, it automatically searches the network for those devices which support the HiDiscovery protocol.

HiDiscovery uses the first PC network card found. If the computer has several network cards, select these in HiDiscovery on the toolbar.

HiDiscovery displays a line for every device which reacts to the HiDiscovery protocol.

HiDiscovery enables the user to identify the devices displayed.

☐ Select a device line.

☐ Click on the signal symbol in the tool bar to set the LEDs for the selected device flashing. To switch off the flashing, click on the symbol again.

☐ By double-clicking a line, open a window to enter the device name and the IP parameters.

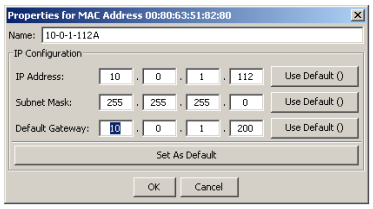


FIGURE 12 – HiDiscovery - assigning IP parameters

Note: When the IP address is entered, the Magnum 12KX copies the local configuration settings.

Note: For security reasons, switch off the HiDiscovery function for the Magnum 12KX in the Web-based interface, after assignig the IP parameters to the Magnum 12KX.

Note: Save the settings so that the entries remain after a restart.

Loading the system configuration from the ACA

The Auto Configuration Adapter (ACA) is a device for

- storing the configuration data of a device and
- storing the device software.

In the case of a device becoming inoperative, the ACA makes it possible to easily transfer the configuration data by means of a substitute device of the same type.

When the Magnum 12KX is started, it checks for an ACA. If it finds an ACA with a valid password and valid software, the Magnum 12KX loads the configuration data from the ACA.

The password is valid if

- the password in the Magnum 12KX matches the password in the ACA or
- the preset password is entered in the Magnum 12KX.

The flow chart explains the ACA load sequence.

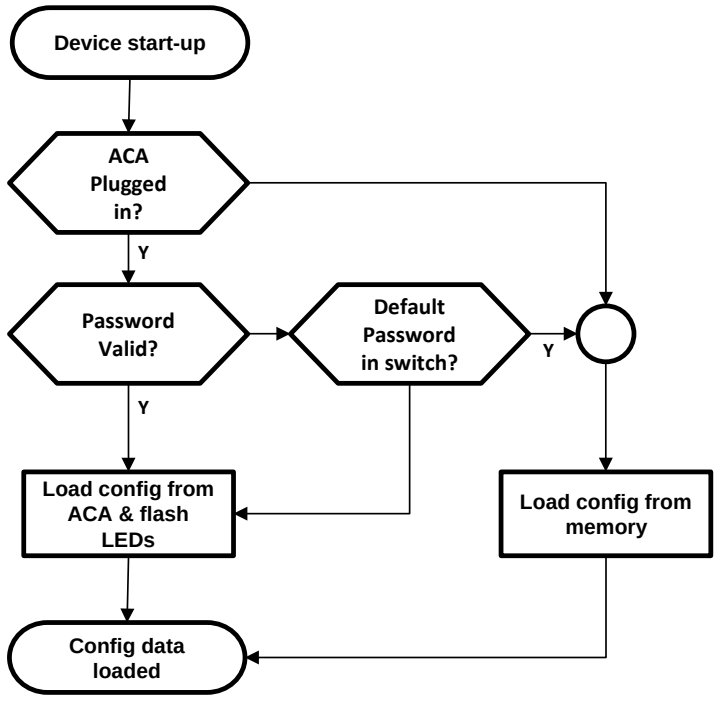


FIGURE 13 – Flow chart of loading configuration data from the ACA.

System configuration via BOOTP

When it is started up via BOOTP (bootstrap protocol), Magnum 12KX receives its configuration data in accordance with the BOOTP process.

Note: In its delivery state, the Magnum 12KX gets its configuration data from the DHCP server.

☐ Activate BOOTP to receive the configuration data, or see the CLI:

`enable`	**Switch to the Privileged EXEC mode.**
`network protocol bootp`	**Activate BOOTP.**
`copy system:running-config nvram:startup-config`	**Activate BOOTP.**
`y`	**Confirm save.**

FIGURE 14 – Sequence of steps to enable BOOTP

☐ Provide the BOOTP server with the following data for a device:

```
# /etc/bootptab for BOOTP-daemon bootpd
#
# gw -- gateway
# ha -- hardware address
# ht -- hardware type
# ip -- IP address
# sm -- subnet mask
# tc -- template

.global:\
:gw=0.0.0.0:\
:sm=255.255.240.0:

switch_01:ht=ethernet:ha=008063086501:ip=10.1.112.83:tc=.global:
switch_02:ht=ethernet:ha=008063086502:ip=10.1.112.84:tc=.global:
```

FIGURE 15 – Example BOOTP file.

Lines that start with a '#' character are comment lines.

The lines under ".global:" make the configuration of several devices easier. With the template (tc) allocate the global configuration data (tc=.global:) to each device .

The direct allocation of hardware address and IP address is performed in the device lines (switch-0...).

☐ Enter one line for each device.
☐ After ha= enter the hardware address of the device.
☐ After ip= enter the IP address of the device.

System Configuration via DHCP

The DHCP (Dynamic Host Configuration Protocol) is a further development of BOOTP, which it has replaced. The DHCP additionally allows the configuration of a DHCP client via a name instead of via the MAC address.

For the DHCP, this name is known as the “client identifier” in accordance with RFC-2131.

The Magnum 12KX uses the name entered under sysName in the system group of the MIB II as the client identifier. The user can enter this system name directly via SNMP, the Web-based management (see system dialog), or the Command Line Interface.

During startup operation, a Magnum 12KX receives its configuration data.

The Magnum 12KX sends its system name to the DHCP server. The DHCP server can then use the system name to allocate an IP address as an alternative to the MAC address.
In addition to the IP address, the DHCP server sends
– the netmask
– the default gateway (if available)
– the tftp URL of the configuration file (if available).

The Magnum 12KX accepts this data as configuration parameters.
If an IP address was assigned by a DHCP server, it will be permanently saved locally.

Option	Meaning
1	Subnet Mask
2	Time Offset
3	Router
4	Time server
12	Host Name
61	Client Identifier
66	TFTP Server Name
67	Bootfile Name

Table 3: DHCP options which the Magnum 12KX requests.

The advantage of using DHCP instead of BOOTP is that the DHCP server can restrict the validity of the configuration parameters (“Lease”) to a specific time period (known as dynamic address allocation). Before this period (“Lease Duration”) elapses, the DHCP client can attempt to renew this lease. Alternatively, the client can negotiate a new lease. The DHCP server then allocates a random free address.

To avoid this, most DHCP servers provide the explicit configuration option of always assigning a specific client the same IP address based on a unique hardware ID (known as static address allocation).

By default, DHCP is activated.

As long as DHCP is activated, the Magnum 12KX attempts to obtain an IP address. If it cannot find a DHCP server after restarting, it will not have an IP address.

To activate/deactivate DHCP use an alternate setup method such as BOOTP.

Note: When using HiVision network management, ensure that DHCP always allocates the same IP address to each device.

In the appendix, there is an example for the configuration of a BOOTP/DHCP server.

Example of a DHCP configuration file:

```
# /etc/dhcpd.conf for DHCP Daemon
#
subnet 10.1.112.0 netmask 255.255.240.0 {
option subnet-mask 255.255.240.0;
option routers 10.1.112.96;
}
#
# Host berta requests IP configuration
# with her MAC address
#
host berta {
hardware ethernet 00:80:63:08:65:42;
fixed-address 10.1.112.82;
}
#
# Host hugo requests IP configuration
# with his client identifier.
#
host hugo {
#
option dhcp-client-identifier "hugo";
option dhcp-client-identifier 00:68:75:67:6f;
fixed-address 10.1.112.83;
server-name "10.1.112.11";
filename "/agent/config.dat";
}
```

FIGURE 16 – Example DHCP configuration file.

Lines that start with a '#' character are comment lines.

The lines preceding the individually listed devices refer to settings that apply to all the following devices.

The fixed-address line assigns a permanent IP address to the Magnum 12KX.

For further information, please refer to the DHCP server manual for the Magnum 12KX acting as a DHCP server.

System Configuration via DHCP Option 82

As with the classic DHCP, on startup an agent receives its configuration data according via BOOTP or DHCP.

While the system configuration is based on the classic DHCP protocol on the device being configured, Option 82 is based on the network topology. This procedure gives the user the option of always assigning the same IP address to any device which is connected to a particular location (port of a device) on the LAN.

The installation of a DHCP server is described later in this manual.

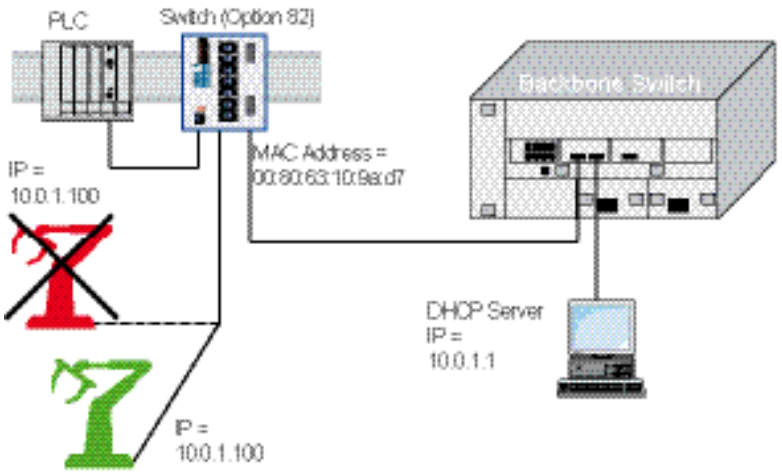


FIGURE 17 – Application example of using Option 82.

Web-based IP Configuration

With the `Basic Settings:Network` dialog define the source from which the Magnum 12KX gets its IP parameters after starting, and assign the IP parameters and VLAN ID as well as configure the HiDiscovery access.

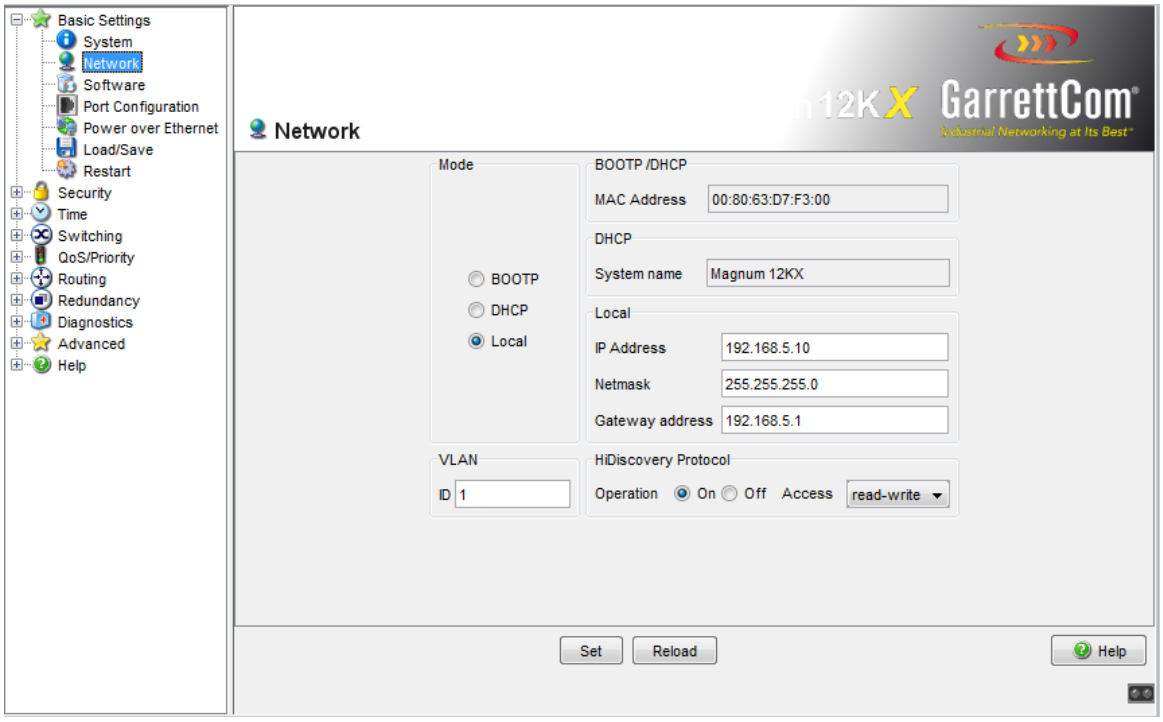


FIGURE 18 – Network Parameters Dialog.

☐ Under “Mode”, enter where the Magnum 12KX gets its IP parameters:

- In the BOOTP mode, the configuration is via a BOOTP or DHCP server on the basis of the MAC address of the Magnum 12KX.
- In the DHCP mode, the configuration is via a DHCP server on the basis of the MAC address or the name of the Magnum 12KX.
- In the “local” mode the net parameters in the Magnum 12KX memory are used.

☐ Enter the parameters on the right according to the selected mode.

☐ Enter the name applicable to the DHCP protocol in the “Name” line in the system dialog of the Web-based interface.

☐ The “VLAN” frame enables user to assign a VLAN to the agent. If 0 is entered here as the VLAN ID (not included in the VLAN standard version), the agent will then be accessible from all VLANs.

☐ The HiDiscovery protocol allows user to allocate an IP address to the Magnum 12KX on the basis of its MAC address. Activate the HiDiscovery protocol an IP address needs to be allocated to the Magnum 12KX using the HiDiscovery protocol (note default settings: operation “on”, Access is set to “read-write”).

Note: Saving the settings ensures that they are preserved after a power failure or restart.

Recovering System Configuration

The Magnum 12KX provides two plug-and-play solutions for recovering system configuration, e.g. when replacing a faulty device with a device of the same type. These two methods are:

- Configuring the new Magnum 12KX using an Auto Configuration Adapter (ACA) or
- configuration via DHCP Option 82

In both cases, when the new device is started, it is given the same configuration data that the replaced device had.

Note: To access the Magnum 12KX via SSH, an SSH key is also needed. To transfer the SSH key of the old device to the new one, the following options exist:

- If the key has already been created and saved external to the device (e.g. on administration workstation), load the saved key onto the new device
- Otherwise create a new SSH key and load it onto the new device. Note that the new device now identifies itself using the new key installed.

Chapter 3

Loading / Saving settings

The Magnum 12KX saves settings such as the IP parameters and the port configuration in the temporary memory. These settings are lost when the device is switched off or rebooted.

Magnum 12KX enables user to

- load settings from a non-volatile memory into the temporary memory
- save settings from the temporary memory in a non-volatile memory.

If the current configuration are changed (for example, by switching a port off), the Web-based interface changes the “load/save” symbol in the navigation tree from a disk symbol to a yellow triangle (see figure below).

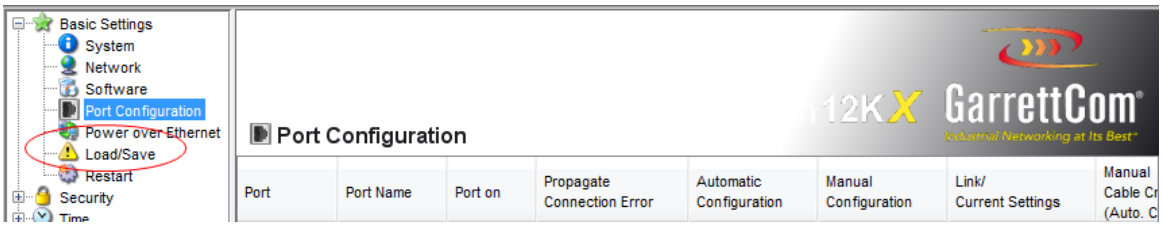


FIGURE 19 – When any changes are made to the configuration, the Load/Save menu changes to a "caution" triangle, as a reminder to save the changes made.

After saving the configuration, the Web-based interface displays the “load/save” symbol as a disk again.

Loading settings

When the Magnum 12KX is restarted, the device loads its configuration data from the local non-volatile memory, provided the user has not activated BOOTP/DHCP and no ACA is connected to the device.

During operation, the Magnum 12KX allows the user to load settings from the following sources:

- the local non-volatile memory
- from the Auto Configuration Adapter. If an ACA is connected to the Magnum 12KX, the device automatically loads its configuration from the ACA during the boot procedure.
- a file in the connected network (setting by default)
- a binary file or an editable and readable script on the PC and
- the firmware (restoration of the configuration by default).

Note: When loading a configuration, do not access the Magnum 12KX until it has loaded the configuration file and has made the new configuration settings.

Note: Depending on the complexity of the configuration settings, this procedure may take 10 to 200 seconds.

Loading from the local non-volatile memory

When loading the configuration data locally, the Magnum 12KX loads the configuration data from the local non-volatile memory if no ACA is connected to the device.

☐ Select the `Basics: Load/Save` dialog.

☐ In the "Load" frame, click "from Device" as shown below

FIGURE 20 – Restoring the configuration from NVRAM (or deleting the running configuration) using the Web interface.

☐ Click "Restore" as shown above

`enable`	**Switch to the Privileged EXEC mode.**
`copy nvram:startup-config system:running-config`	**The Magnum 12KX loads the configuration data from the local non-volatile memory.**

FIGURE 21 – Restoring the configuration from NVRAM (or deleting the running configuration) using CLI

Loading from the Auto Configuration Adapter

If a ACA is connected to the Magnum 12KX, the device automatically loads its configuration from the ACA during the boot procedure.

Note: The Magnum 12KX allows the user to trigger the following events when the configuration stored on the ACA does not match that in the device:

- an alarm (trap) is sent,
- the device status is updated,
- the status of the signal contacts is updated.

Loading from a file

The Magnum 12KX allows the user to load the configuration data from a file in the connected network if there is no Auto Configuration Adapter connected to the device.

☐ Select the `Basics: Load/Save` dialog.

☐ In the "Load" frame, click

- "from URL" if the user wants the Magnum 12KX to load the configuration data from a file and retain the locally saved configuration.
- "from URL & save to Device" if the user wants the Magnum 12KX to load the configuration data from a file and save this configuration locally.
- "via PC" if the user want the Magnum 12KX to load the configuration data from a file from the PC and retain the locally saved configuration.

☐ In the "URL" frame, enter the path under which the Magnum 12KX will find the configuration file, if the user wants to load from the URL.

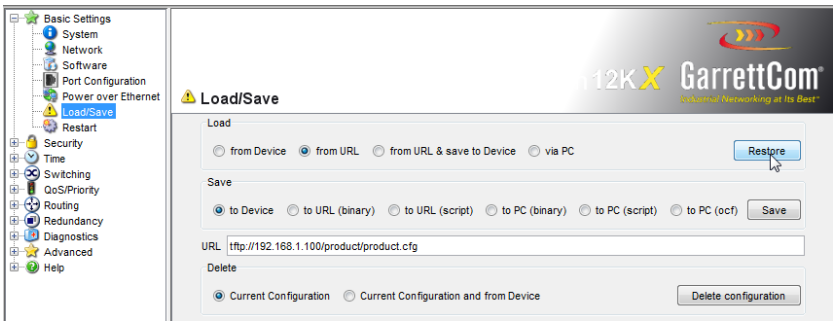


FIGURE 22 – Loading the configuration from a file. Note, select URL and then type in the information of the URL from where the file is restored.

☐ Click "Restore".

The URL identifies the path to the tftp server from which the Magnum 12KX loads the configuration file. The URL is in the format

tftp://IP address of the tftp server/path name/file name

(e.g. `tftp://10.1.112.5/switch/config.dat`).

`enable` **Switch to the Privileged EXEC mode.**

```
copy
tftp://10.1.112.159/switch/config.
dat nvram:startup-config
```

The loads the configuration data from a tftp server in the connected network.

FIGURE 23 – Loading configuration using the CLI.

Note: The loading process started by DHCP/BOOTP shows the selection of "from URL & save locally" in the "Load" frame. If an error message appears when saving a configuration, it could be due to an active loading process. DHCP/BOOTP only finishes a loading process when a valid configuration has been loaded. If DHCP/BOOTP does not find a valid configuration, then finish the loading process by loading the local configuration in the "Load" frame.

Resetting to factory defaults

To reset the Magnum 12KX to factory default settings, use the Delete dialog as shown below.

☐ Select the `Basics: Load/Save` dialog.

☐ Make selection in the "Delete" frame.

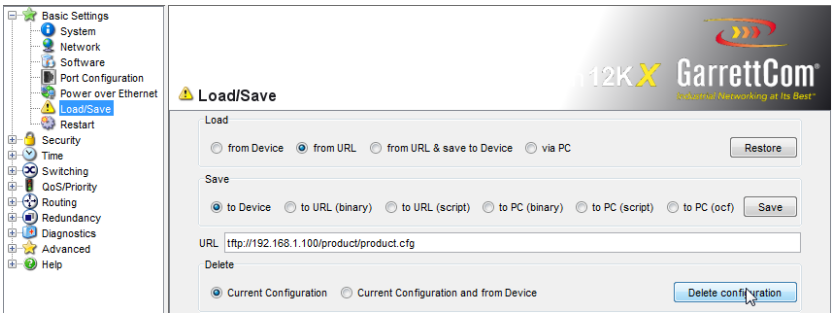


FIGURE 24 – Deleting the configuration. Selecting "Current Configuration" resets the running configuration. Selecting "Current Configuration and from Device" resets both the startup or saved configuration as well as running configuration.

☐ Click "Delete configuration" after making the selection as shown above.

Setting in the system monitor

☐ Select 5 “Erase main configuration file”

This menu item allows user to reset the Magnum 12KX to its state by default. The Magnum 12KX saves configurations other than the original one in its Flash memory in the configuration file `*.cfg`.

☐ Press the Enter key to delete the configuration file.

Saving settings

In the "Save" frame, the user has the option to

- save the current configuration on the Magnum 12KX
- save the current configuration in binary form in a file under the specified URL, or as an editable and readable script
- save the current configuration in binary form or as an editable and readable script on the PC.

Saving locally (and on the ACA)

The Magnum 12KX allows the user to save the current configuration data in the local non-volatile memory and the ACA.

☐ Select the `Basics: Load/Save` dialog.

☐ In the “Save” frame, click “to Device” as shown below

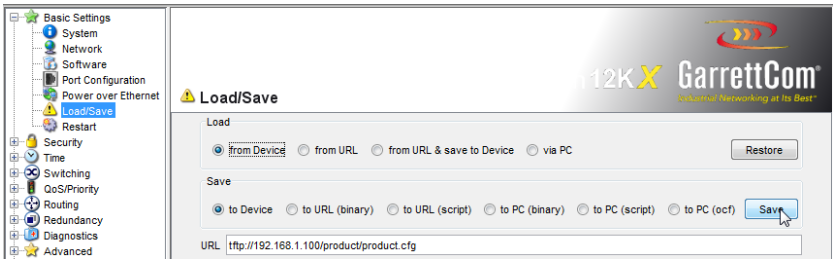


FIGURE 25 – Saving configuration locally. If an ACA is plugged in, it will also be updated.

☐ Click on “Save”.
The Magnum 12KX saves the current configuration data in the local non-volatile memory and, if an ACA is connected, also in the ACA.

`enable`	**Switch to the Privileged EXEC mode.**
`copy system:running-config nvram:startup-config`	**The Magnum 12KX saves the current configuration data in the local non-volatile memory and, if an ACA is connected, also on the ACA.**

FIGURE 26 – Saving configuration locally using CLI. If an ACA is plugged in, it will also be updated.

Note: After successfully saving the configuration on the Magnum 12KX, an alarm (trap) `ConfigurationSavedTrap` is sent together with the information about the Auto Configuration Adapter (ACA), if one is connected.

Note: The Magnum 12KX allows the user to trigger the following events when the configuration stored on the ACA does not match that in the device:

- an alarm (trap) is sent
- the device status is updated
- the status of the signal contacts is updated

Saving to a file on URL

Magnum 12KX allows the user to save the current configuration data in a file in the connected network.

Note: The configuration file includes all configuration data, including the password. Please ensure that the tftp server is secured.

☐ Select the `Basics: Load/Save` dialog.

☐ In the “Save” frame, click “to URL (binary)” to receive a binary file, or “to URL (script)” to receive an editable and readable script.

☐ In the “URL” frame, enter the path under which user wants the configuration file.

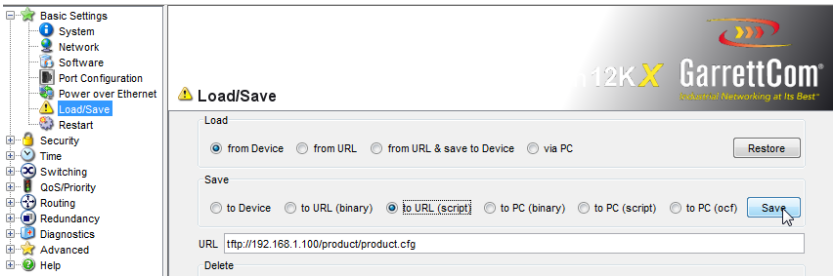


FIGURE 27 – Saving a script file (as shown above).

The URL identifies the path to the tftp server on which the Magnum 12KX saves the configuration file. The URL is in the format

tftp://IP address of the tftp server/path name/file name

(e.g. tftp://10.1.112.5/switch/config.dat).

☐ Click "Save" as shown above.

`enable`	**Switch to the Privileged EXEC mode.**
`copy nvram:startup-config tftp://10.1.112.159/switch/config.dat`	**The Magnum 12KX saves the configuration data in a binary file on a tftp server in the connected network.**
`copy nvram:script tftp://10.0.1.159/switch/config.txt`	**The Magnum 12KX saves the configuration data in a script file on a tftp server in the connected network.**

FIGURE 28 – Saving configuration locally using CLI. If an ACA is plugged in, it will also be updated

Saving a file locally on the PC

Magnum 12KX allows the user to save the current configuration data in a binary file on PC.

☐ Select the `Basics: Load/Save` dialog.

☐ In the "Save" frame, click "on the PC (binary)".

FIGURE 29 – Saving the **CONFIGURATION** locally to the PC. After clicking "Save" a dialog box is opened, allowing the file to be saved in the proper folder. Note the example above saves the configuration as a script (text) file. The configuration can also be saved as a binary file.

☐ In the save dialog, enter the name of the file wherethe Magnum 12KX should save the configuration file.

☐ Click "Save".

Chapter 4

Updating Software

Magnum 12KX device software can be updated. Software updates are essential to take advantage of bug fixes as well as take advantage of new features added to the software.

Checking the software releases

To check for the software release, follow the steps shown below.

☐ Select the `Basics:Software` dialog.

☐ This dialog shows the variant, the release number and the date of the software saved on the Magnum 12KX.

- "Stored Version": the software in the non-volatile memory
- "Running Version": the software currently being used
- "Backup Version": the backup software in the non-volatile memory

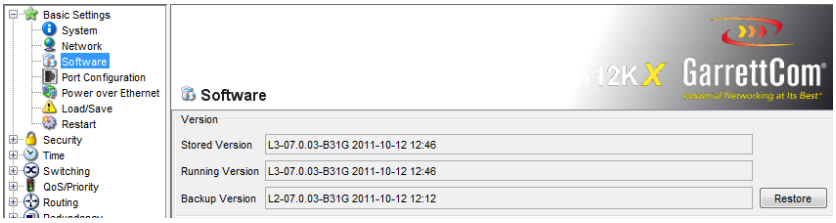


FIGURE 30 – Displaying the software version.

`enable`	**Switch to the Privileged EXEC mode.**
`show sysinfo`	**Display the system information.**

```
Last Alarm 1.............................. Failure of Power Supply 2
Alarm 2.................................... None
System Description..................... Magnum 12KX Gigabit Switch
System Name................................ Magnum 12KX
System Location............................ Fremont, CA
System Contact........................... support@garrettcom.com
System Up Time........................... 0 days 4 hrs 11 mins 23 secs
System Date and Time (local time zone)..... 2011-10-23 22:22:20
System IP Address.......................... 192.168.5.10
Boot Software Release...................... 07.0.00-tst
Boot Software Build Date................... 2011-04-26 10:09
Running Software Release................... L3-07.0.03-B31G
Running Software Build Date................ 2011-10-12 12:46
Stored Software Release.................... L3-07.0.03-B31G
Stored Software Build Date................. 2011-10-12 12:46
Backup Software Release.................... L2-07.0.03-B31G
Backup Software Build Date................. 2011-10-12 12:12
Backplane Hardware Revision................ 1.10 / 15 / 0202
Serial Number (Backplane).................. 942004999010501793
Base MAC Address (Backplane)............... 00:80:63:d7:f3:00
Number of MAC Addresses (Backplane)........ 256 (0x100)
Configuration state........................ Not in sync.
Auto Configuration Adapter, State.......... Not present
Power Supply P1, State..................... Present
Power Supply P2, State..................... Failed
Media Module Information: MAG1240-4C4C4C4C9999TMMHRHH
CPU Utilization............................ 20%
Average CPU Utilization.................... 15%
Flashdisk (Kbytes free).................... 5959
```

FIGURE 31 – Displaying the software version using CLI.

Loading the software

The Magnum 12KX gives four options for loading the software:

- manually from the ACA (out-of-band),
- automatically from the ACA (out-of-band),
- via TFTP from a tftp server (in-band) and
- via a file selection dialog from the PC.

Note: The existing configuration of the Magnum 12KX is still present after the new software is installed.

Loading the Software manually from the ACA

Connect the ACA 21-USB to a USB port of the PC like a conventional USB stick and copy the Magnum 12KX software into the main directory of the ACA 12-USB.

☐ Connect the ACA onto which the Magnum 12KX software was copied with the USB port of the Magnum 12KX.

☐ Open the system monitor.

☐ Select 2 and press the Enter to copy the software from the ACA 21-USB into the local memory of the Magnum 12KX. At the end of the update, the system monitor asks to press any key to continue.

☐ Select 3 to start the new software on the Magnum 12KX.

The system monitor offers additional options in connection with the software on the Magnum 12KX:

- selecting the software to be loaded
- starting the software
- performing a cold start

Selecting the software to be loaded

In this menu item of the system monitor, select one of two possible software releases that are to be loaded. The following window appears on the screen:

```
Select Operating System Image

(Available OS: Selected: 05.0.00 (2009-08-07 06:05), Backup: 04.2.00
(2009-07-06 06:05 (Locally selected: 05.0.00 (2009-08-07 06:05))

1  Swap OS images
2  Copy image to backup
3  Test stored images in Flash mem.
4  Test stored images in USB mem.
5  Apply and store selection
6  Cancel selection
```

FIGURE 32 – Loading software using system monitor.

The choices are:

SWAP OS IMAGES

The memory of the Magnum 12KX provides space for two images of the software. This provides the ability to load a new version of the software without deleting the existing version.

☐ Select 1 to load the other software in the next booting process.

COPY IMAGE TO BACKUP

☐ Select 2 to save a copy of the active software.

TEST STORED IMAGES IN FLASH MEMORY

☐ Select 3 to check whether the images of the software stored in the flash memory contain valid codes.

TEST STORED IMAGES IN USB MEMORY

☐ Select 4, to check whether the images of the software stored in the ACA 21-USB contain valid codes.

APPLY AND STORE SELECTION

☐ Select 5 to confirm the software selection and to save it.

CANCEL SELECTION

☐ Select 6 to leave this dialog without making any changes.

Starting the software

This menu item (Start Selected Operating System) of the system monitor allows user to start the software selected.

Performing a cold start

This menu item (End (reset and reboot)) of the system monitor allows user to reset the hardware of the Magnum 12KX and perform a restart.

Automatic software update by ACA

☐ For a software update via the ACA, first copy the new Magnum 12KX software into the main directory of the Auto Configuration Adapter. If the version of the software on the ACA is newer or older than the version on the Magnum 12KX, it performs a software update.

Note: Software versions with release 06.0.00 and higher in the non-volatile memory of the Magnum 12KX support the software update via the ACA. If the Magnum 12KX software is older, the user has the option of loading the software manually from the ACA.

☐ Give the file the name that matches the device type and the software variant, e.g. rsL2P.bin for device type RS2 with the software variant L2P. Please note the case-sensitivity here.
If the software was copied from a CD-ROM or from a Web server of the manufacturer, the software already has the correct file name.

☐ Also create an empty file with the name “autoupdate.txt” in the main directory of the ACA. Please note the case-sensitivity here.

☐ Connect the Auto Configuration Adapter to the Magnum 12KX and restart it.

☐ The Magnum 12KX automatically performs the following steps:
- During the booting process, it checks whether an ACA is connected.
- It checks whether the ACA has a file with the name “autoupdate.txt” in the main directory.
- It checks whether the ACA has a software file with a name that matches the device type in the main directory.
- If compares the software version stored on the ACA with the one stored on the device.
- If these conditions are fulfilled, the Magnum 12KX loads the software from the ACA to its non-volatile memory as the main software.
- The Magnum 12KX keeps a backup of the existing software in the non-volatile memory.
- The Magnum 12KX then performs a cold start, during which it loads the new software from the non-volatile memory.

One of the following messages in the log file indicates the result of the update process:
- S_watson_AUTOMATIC_SWUPDATE_SUCCESSFUL: Update completed successfully.
- S_watson_AUTOMATIC_SWUPDATE_FAILED_WRONG_FILE: Update failed. Reason: incorrect file.
- S_watson_AUTOMATIC_SWUPDATE_FAILED_SAVING_FILE: Update failed. Reason: error when saving.

☐ In the browser, click on “Reload” to use the Web-based interface to access the Magnum 12KX again after it is booted.

Loading the software from the tftp server

For a tftp update, a tftp server is needed. The tftp server also needs to be configured to respond to tftp requests made by the Magnum12KX.

The updates can be done via the web or the CLI.

☐ Select the `Basics:Software` dialog.

The URL identifies the path to the software stored on the tftp server. The URL is in the format tftp://IP address of the tftp server/path name/file name

(e.g. `tftp://192.168.1.1/device/device.bin`).

☐ Enter the path of the Magnum 12KX software.

☐ Click on "Update" to load the software from the tftp server to the Magnum 12KX.

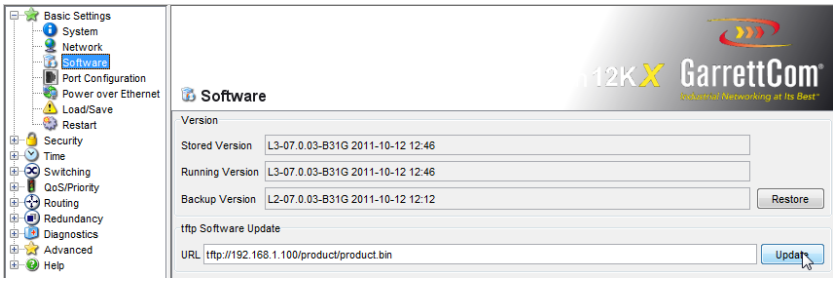


FIGURE 33 – Software update dialog.

☐ After successfully loading it, activate the new software: Select the dialog `Basic Settings:Restart` and perform a cold start.
In a cold start, the Magnum 12KX reloads the software from the non-volatile memory, restarts, and performs a self-test.

FIGURE 34 – Resetting Magnum 12KX after software update.

☐ After booting the Magnum 12KX, refresh the browser or click "Reload" in the browser to access the device again.

`enable`	**Switch to the Privileged EXEC mode.**
`copy tftp://10.0.1.159/rsL2E.bin system:image`	**Transfer the "rsL2E.bin" software file to the Magnum 12KX from the tftp server with the IP address 10.0.1.159.**
`reboot`	**Reset the switch (cold start).**

FIGURE 35 – CLI commands to update software using tftp

Loading the Software via File Selection

For an HTTP software update (via a file selection window), the Magnum 12KX software must be on a data carrier that can be accessed via a file selection window from the workstation.

☐ Select the `Basics:Software` dialog.
☐ In the file selection frame, click on "...".
☐ In the file selection window, select the Magnum 12KX software (name type: *.bin, e.g. device.bin) and click on "Open".

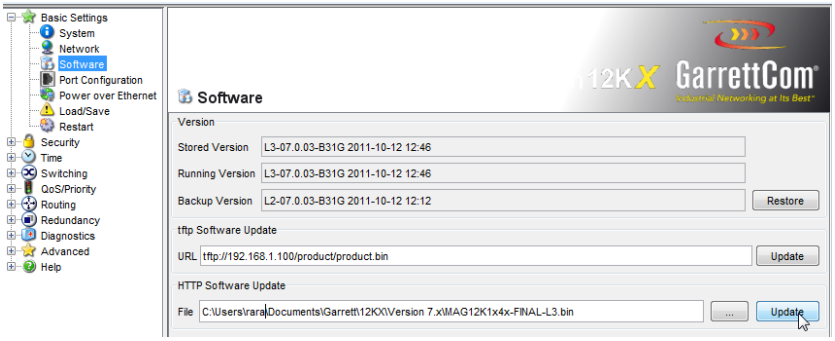


FIGURE 36 – Using the browser to select file to upload.

☐ Click on "Update" to transfer the software to the Magnum 12KX.

The end of the update is indicated by one of the following messages:
- Update completed successfully.
- Update failed. Reason: incorrect file.

- Update failed. Reason: error when saving.
- File not found (reason: file name not found or does not exist).
- Connection error (reason: path without file name).

☐ After the update is completed successfully, activate the new software by doing a cold start as shown in the prior section.

☐ In a cold start, the Magnum 12KX reloads the software from the non-volatile memory, restarts, and performs a self-test.

☐ After booting the Magnum 12KX, refresh the browser or click "Reload" in the browser to access the device again.

Chapter 5

Configuring the Ports

The port configuration consists of:

- Switching the port on and off
- Selecting the operating mode
- Activating the display of connection error messages
- Configuring Power over ETHERNET.

Port Management (Configuration)

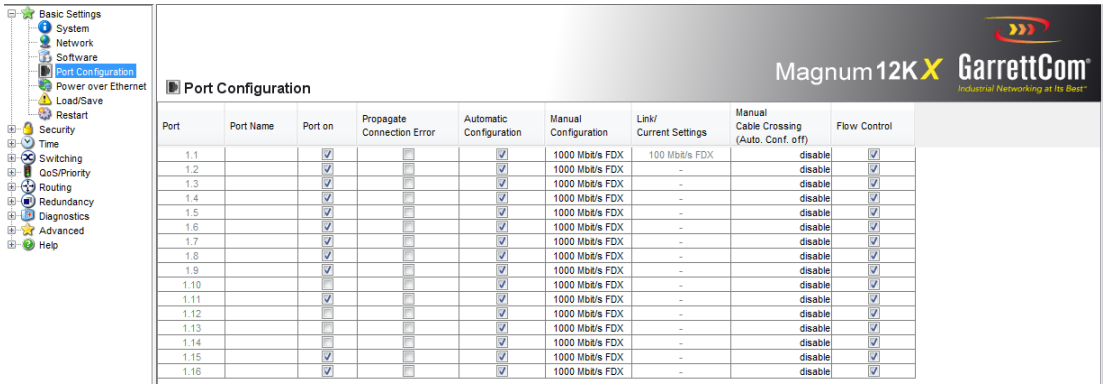
The next few sections looks at how the ports can be managed for additional security.

Switching the port on and off

By default, all the ports are on. For a higher level of security, it is recommended to switch off all the ports which are not in use. This can be done as shown below.

☐ Select the `Basics:Port Configuration` dialog.

☐ In the "Port on" column, check the boxes for the ports that are connected to another device. The unchecked boxes disable the ports. Remember to click on "Set" when completed.



Port	Port Name	Port on	Propagate Connection Error	Automatic Configuration	Manual Configuration	Link/ Current Settings	Manual Cable Crossing (Auto. Conf. off)	Flow Control
1.1		☑	☐	☑	1000 Mbit/s FDX	100 Mbit/s FDX	disable	☑
1.2		☑	☐	☑	1000 Mbit/s FDX	-	disable	☑
1.3		☑	☐	☑	1000 Mbit/s FDX	-	disable	☑
1.4		☑	☐	☑	1000 Mbit/s FDX	-	disable	☑
1.5		☑	☐	☑	1000 Mbit/s FDX	-	disable	☑
1.6		☑	☐	☑	1000 Mbit/s FDX	-	disable	☑
1.7		☑	☐	☑	1000 Mbit/s FDX	-	disable	☑
1.8		☑	☐	☑	1000 Mbit/s FDX	-	disable	☑
1.9		☑	☐	☑	1000 Mbit/s FDX	-	disable	☑
1.10		☐	☐	☑	1000 Mbit/s FDX	-	disable	☑
1.11		☑	☐	☑	1000 Mbit/s FDX	-	disable	☑
1.12		☐	☐	☑	1000 Mbit/s FDX	-	disable	☑
1.13		☐	☐	☑	1000 Mbit/s FDX	-	disable	☑
1.14		☐	☐	☑	1000 Mbit/s FDX	-	disable	☑
1.15		☑	☐	☑	1000 Mbit/s FDX	-	disable	☑
1.16		☑	☐	☑	1000 Mbit/s FDX	-	disable	☑

FIGURE 37 – Enabling and disabling ports. In this example, ports 10, 12,13,14 are disabled. All other ports are enabled.

Selecting the operating mode

By default, all the ports are set to the “Automatic configuration” operating mode.

Note: The active automatic configuration has priority over the manual configuration.

☐ Select the `Basics:Port Configuration` dialog.

☐ If the Magnum 12KX connected to this port requires a fixed setting
– select the operating mode (transmission rate, duplex mode) in the "Manual configuration" column and
– deactivate the port in the "Automatic configuration" column.

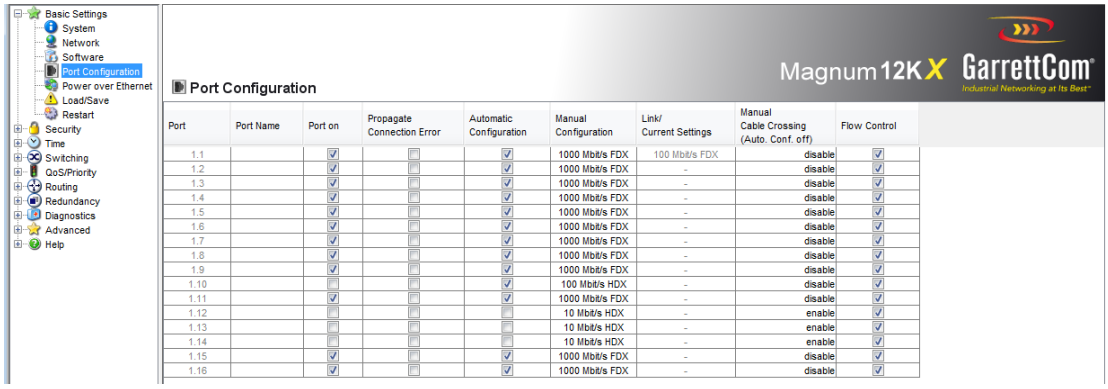


FIGURE 38 – Changing the auto configuration capability of the ports. In this example, for ports 12-14, the speed as well as the MDI-MDI-X auto sensing is disabled. For port 10, only the speed is set.

Displaying connection error messages

By default, the Magnum 12KX displays connection errors via the signals being sent or propagated. If a link alarm is to be suppressed, uncheck the box as shown below. To propagate the alarm to the 12KX switch, check the box as shown below.

Select the Basics:Port Configuration dialog.

☐ In the "Propagate connection error" column, select the ports for which link monitoring is needed.

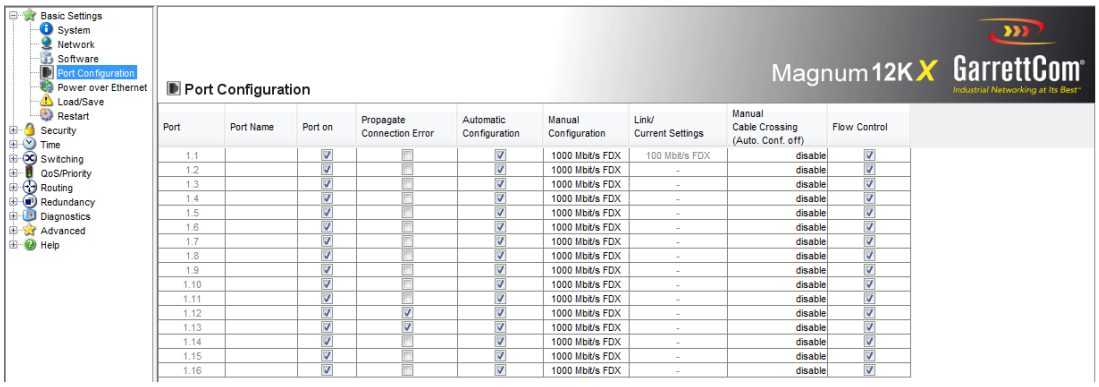


FIGURE 39 – Propagating link alarms and connection error information. In the above example, ports 12 and 13 are enabled to do that.

Configuring Power over Ethernet (PoE)

If the Magnum 12KX is purchased with the PoE options, the first four ports can provide Power over Ethernet (PoE) to devices such as VoIP phones, access points, security and surveillance cameras and other devices. PoE is compliant to the IEEE 802.3af standard. By default, the PoE function is activated on all PoE capable ports.

☐ Select the `Basics:Power over Ethernet` dialog.

☐ With “Function on/off” turn the PoE on or off.
☐ With “Send Trap” the Magnum 12KX can send a trap in the following cases:
  – If a value exceeds/falls below the performance threshold.
  – If the PoE supply voltage is switched on/off for at least one port.
☐ Enter the power threshold in “Threshold”. When this value is exceeded/not achieved, the Magnum 12KX will send a trap, provided that “Send Trap” is enabled. For the power threshold enter the power yielded as a percentage of the nominal power.
☐ “Nominal Power” displays the power that the Magnum 12KX nominally provides for all PoE ports together.
☐ “Reserved Power” displays the maximum power that the Magnum 12KX provides to all the connected PoE devices together on the basis of their classification.
☐ “Delivered Power” shows how large the current power requirement is at all PoE ports.

The difference between the "nominal" and "reserved" power indicates how much power is still available to the free PoE ports.

- ☐ In the “POE on” column, enable/disable PoE at this port.
- ☐ The “Status” column indicates the PoE status of the port.
- ☐ The “Class” column shows the class of the connected device:

  Class Maximum power delivered
  0: 15.4 W = state by default
  1: 4.0 W
  2: 7.0 W
  3: 15,4 W
  4: reserved, treat as class 0
- ☐ The “Name” column indicates the name of the port, see `Basic settings:Port configuration`.

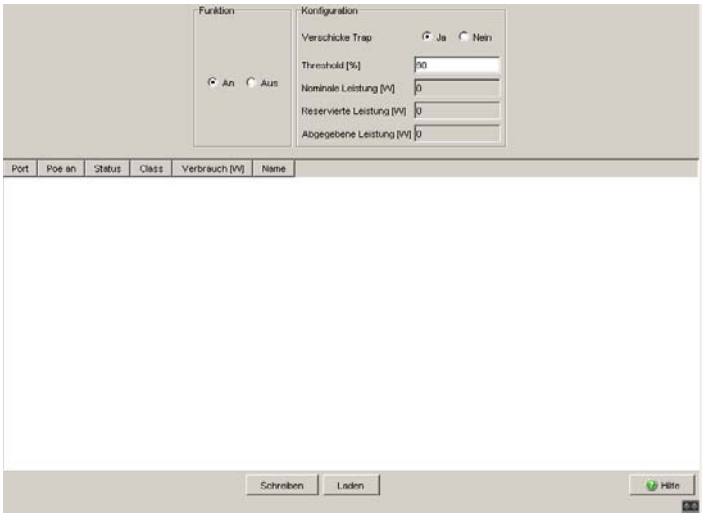


FIGURE 40 – Power over Ethernet dialog.

Chapter 6

Security Considerations

The Magnum 12KX provides the following functions to help protect it against unauthorized access.

- Password for SNMP access
- Telnet/Web/SSH access disabling
- Restricted management access
- HiDiscovery function disabling
- Port access control via IP or MAC address
- Port authentication according to IEEE 802.1X
- Access Control Lists (ACL).

Protecting the Magnum 12KX

To maximize the protection of the Magnum 12KX against unauthorized access in just a few steps, perform some or all of the following steps:

☐ Deactivate SNMPv1 and SNMPv2 and select a password for SNMPv3 access other than the standard password.

☐ Deactivate Telnet access.

☐ Deactivate web access after downloading the applet for the web-based interface onto the management station. Start the web-based interface as an independent program and thus have SNMP access to the Magnum 12KX. If necessary, deactivate SSH access. Note - if telnet is deactivated, web and SSH access, the only method to access the Magnum 12KX is via the console.

☐ Deactivate HiDiscovery access.

Note: Make sure to retain at least one option to access the Magnum 12KX. V.24 access is always possible and it cannot be deactivated.

Password for SNMP access

SNMP is enabled by default and is recommended to change the SNMP access password as described below.

Description of password for SNMP access

A network management station communicates with the Magnum 12KX via the Simple Network Management Protocol (SNMP). Every SNMP packet contains the IP address of the sending computer and the password with which the sender of the packet wants to access the device MIB.

The Magnum 12KX receives the SNMP packet and compares the IP address of the sending computer and the password with the entries in the device MIB.

If the password has the appropriate access right, and if the IP address of the sending computer has been entered, then the Magnum 12KX will allow access.

By default, the Magnum 12KX is accessible via the password "public" (read only) and "private" (read and write) to every computer.

To help protect the Magnum 12KX from unwanted access:

☐ First define a new password with read/write privileges.

☐ Treat this password as confidential.

☐ Replace the default "private" password with the confidential password.

☐ Also recommend that the same process is followed for the read or "public" password.

Entering the password for SNMP access

For SNMP v3 Access

☐ Select the `Security:Password/SNMP Access` dialog.

This dialog gives the option of changing the read and read/write passwords for access to the Magnum 12KX via the Web-based interface, via the CLI, and via SNMPv3 (SNMP version 3). Please note that passwords are case-sensitive.

Set different passwords for the read password and the read/write password so that a user that only has read access (user name “user”) does not know, or cannot guess, the password for read/write access (user name “admin”).

If idserentical passwords are set, when the user attempts to write this data the Magnum 12KX reports a general error.

The Web-based interface and the user interface (CLI) use the same passwords as SNMPv3 for the users “manager” and “operator”.

☐ Select “Modify Read-Only Password (User)” to enter the read password.
  ☐ Enter the new read password in the “New Password” line and repeat the entry in the “Please retype” line.

☐ Select “Modify Read-Write Password (Admin)” to enter the read/write password.
  ☐ Enter the read/write password and repeat the entry.

☐ "Data encryption" encrypts the data of the Web-based management that is transferred between the PC and the Magnum 12KX with SNMPv3. Set the "Data encryption" differently for access with a read password and access with a read/write password.

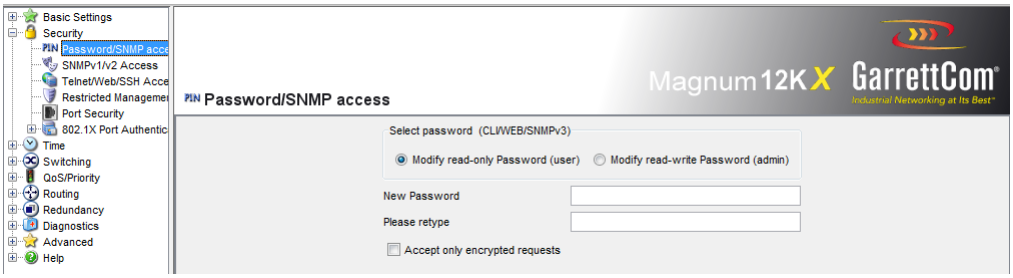


FIGURE 41 – Password/SNMP v3 Access dialog

Note: If the user does not know a password with "read/write" access, they will not have write access to the Magnum 12KX.

Note: For security reasons, the Magnum 12KX does not display the passwords. Make a note of every change. The Magnum 12KX cannot be accessed without a valid password.

Note: For security reasons, SNMPv3 encrypts the password. With the "SNMPv1" or "SNMPv2" setting in the dialog `Security:SNMPv1/v2 access`, the Magnum 12KX transfers the password unencrypted, so that this can also be read.

Note: Use between 5 and 32 characters for the password in SNMPv3, since many applications do not accept shorter passwords.

For SNMP v2 Access

☐ Select the `Security:SNMPv1/v2` access dialog.
With this dialog user can select the access via SNMPv1 or SNMPv2. By default, both protocols are activated. The Magnum 12KX can thus be managed with HiVision or other network management software and communicate with earlier versions of SNMP.

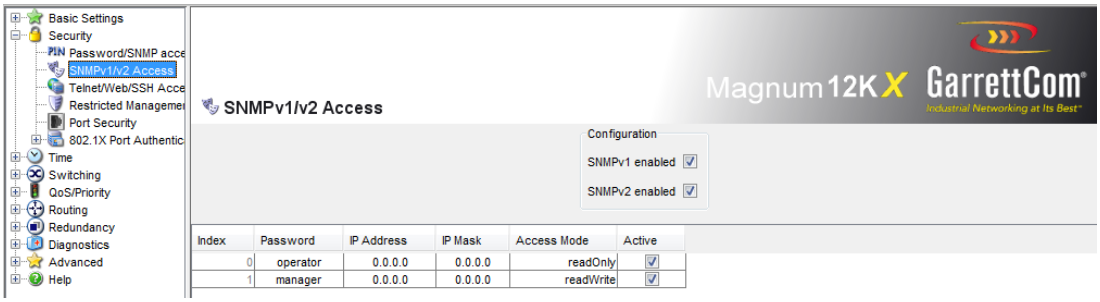


FIGURE 42 – SNMP v1 and v2 access dialog

If SNMPv1 or SNMPv2 has been checked, it can be specified in the table via which IP addresses can access the switch, and what kinds of passwords are to be used.

An IP/netmask of 0.0.0.0 indicates any device can access the switch.

Up to 8 entries can be made in the table.

For security reasons, the read password and the read/write password must not be identical.

Please note that passwords are case-sensitive.

The fields are as follows:

Index	Serial number for this table entry
Password	Password with which this computer can access the Magnum 12KX. This password is independent of the SNMPv2 password.
IP address	IP address of the computer that can access the Magnum 12KX.
IP mask	IP mask for the IP address
Access mode	The access mode determines whether the computer has read-only or read-write access.
Active	Enable/disable this table entry.

To add an entry, click on "Create". To remove an entry click on "Remove"

FIGURE 43 – Adding or deleting entries in the SNMP managed station table.

Telnet/Web/SSH Access

The Magnum 12KX can be accessed using Telnet, SSH as well as the Web interface.

Description of Telnet Access

The Telnet server of the device allows user to configure the Magnum 12KX by using the Command Line Interface (in-band). The Telnet server can be deactivated if Telnet access to the Magnum 12KX is not needed.

By default, the server is enabled.

After the Telnet server has been deactivated, the Magnum 12KX can no longer be accessed via a new Telnet connection. If a Telnet connection already exists, it is kept.

Note: The Command Line Interface (out-of-band) and the `Security:Telnet/Web access` dialog in the Web-based interface allows reactivation of the Telnet server.

Telnet timeout can be changed by the command telnetcon timeout <1-160> where the time (between 1 to 160) is in minutes.

Description of Web Access

The Web server of the Magnum 12KX allows the user to configure the device by using the Web-based interface. Deactivate the Web server if the Magnum 12KX does not need to be accessed from the Web.

By default, the Web server is activated.

After the Web server has been switched off, it is no longer possible to log in via a Web browser. The login to the currently open browser window remains active. Once the browser is closed or the user logs out, the session is prevented.

Description of SSH Access

The SSH server of the Magnum 12KX allows the user to configure the Magnum 12KX by using the Command Line Interface (in-band). The SSH server can be deactivated to disable SSH access to the Magnum 12KX.

By default, the server is deactivated.

After the SSH server has been deactivated, the Magnum 12KX can no longer be accessed via a new SSH connection. If an SSH connection already exists, it is kept.

Note: The Command Line Interface (out-of-band) and the `Security:Telnet/Web access` dialog in the Web-based interface allows the user to reactivate the SSH server.

Note: To be able to access the device via SSH, a key is needed, which has to be installed on the Magnum 12KX (see the "Basic Configuration" user manual).

Enabling/disabling Telnet/Web/SSH Access

☐ Select the `Security:Telnet/Web/SSH access` dialog.

☐ Disable the server to which access should be refused.

FIGURE 44 – Enabling / disabling Telnet, Web, SSH access.

`enable`	**Switch to the Privileged EXEC mode.**
`configure`	**Switch to the Configuration mode.**
`lineconfig`	**Switch to the configuration mode for CLI.**
`transport input telnet`	**Enable Telnet server.**
`no transport input telnet`	**Disable Telnet server.**
`exit`	**Switch to the Configuration mode.**
`ip http server`	**Enable Web server.**
`no ip http server`	**Disable Web server.**
`ip ssh`	**Enable SSH function on Switch**
`no ip ssh`	**Disable SSH function on Switch**

FIGURE 45 – Enabling / disabling Telnet, Web, SSH access using CLI.

Restricted Management Access

The Magnum 12KX allows the user to differentiate the management access to the Magnum 12KX based on IP address ranges, and to differentiate these based on management services (http, snmp, telnet, ssh). This allows managers to define management VLANs or networks from which management of devices are allowed. This capability also allows a manager to define a range of networks as well as stations which can access the switch.

This function can be configured using the Web-based interface or the CLI. The Web-based interface provides the user with an easy configuration option. Make sure the access to the Magnum 12KX is not unintentionally blocked. The CLI access to the Magnum 12KX via V.24 provided at all times is excluded from the function and cannot be restricted.

In the following example, the Management network has the address range 192.168.1.0/24 and the remote access is from a network with the IP address range 109.237.176.0 - 109.237.176.255.

The management policy is to manage devices using SSH from remote network and SNMP/HTTP from the Management network. The parameters thus are:

Parameter	Value
Management network address	192.168.1.0
Management network netmask	255.255.255.0
Desired management access from the Management network	http, snmp
Remote network address	109.237.176.0
Remote network netmask	255.255.255.0
Desired management access from the remote network	ssh

Table 4: Example parameter for the restricted management access

☐ Select the `Security:Restricted Management` dialog.

☐ Create the entries for Management network as well as remote network as shown below.

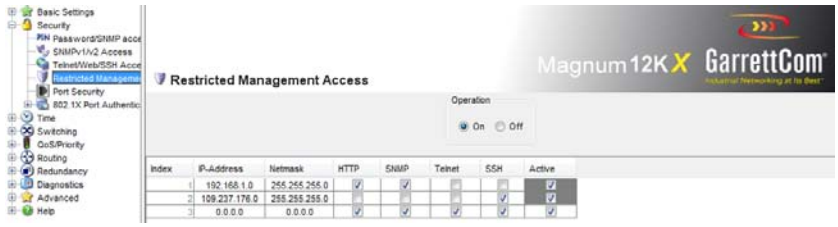


FIGURE 46 – Setting up Management and local access as described above.

Note: Once activated, access to the switch may be terminated. Only way to reset the access is to access the switch via the console or the networks configured.

`enable`	**Switch to the Privileged EXEC mode.**
`show network mgmt-access`	**Display the current configuration.**
`network mgmt-access add`	**Create an entry for the Management network. This is given the smallest free ID in the example, 2.**
`network mgmt-access modify 2 ip 192.168.1.0`	**Set the IP address of the entry for the Management network.**
`network mgmt-access modify 2 netmask 255.255.255.0`	**Set the netmask of the entry for the Management network.**
`network mgmt-access modify 2 telnet disable`	**Deactivate telnet for the entry of the Management network.**
`network mgmt-access modify 2 ssh disable`	**Deactivate SSH for the entry of the Management network.**
`network mgmt-access add`	**Create an entry for the remote network. In the example, this is given the ID 3.**
`network mgmt-access modify 3 ip 109.237.176.0`	**Set the IP address of the entry for the remote network.**
`network mgmt-access modify 3 netmask 255.255.255.0`	**Set the netmask of the entry for the remote network.**
`network mgmt-access modify 3 http disable`	**Deactivate http for the entry of the remote network.**
`network mgmt-access modify 3 snmp disable`	**Deactivate snmp for the entry of the remote network.**
`network mgmt-access modify 3 telnet disable`	**Deactivate telnet for the entry of the remote network.**
`network mgmt-access status 1 disable`	**Deactivate the preset entry.**
`network mgmt-access operation enable`	**Activates the function immediately.**
`show network mgmt-access`	**Display the current configuration of the function.**
`copy system:running-config nvram:startup-config`	**Save the entire configuration in the non-volatile memory.**

FIGURE 47 – Setting up Management and local access as described above using CLI.

HiDiscovery Access

HiDiscovery is a Layer 2 discovery protocol used by the HiVision network management software. HiDiscovery is also used for configuring devices with an IP address or other parameters. Note that for doing that, it is recommended that the Magnum 12KX switch and the HiDiscovery configuration management station are located on the same segment. In theory, they could be on different Ethernet segments. Please ensure that BPDU's are allowed to be propagated in the network if the devices are on different segments.

It is important to disable HiDiscovery after the switch is configured to prevent someone from changing the IP address of the switch.

Description of the HiDiscovery Protocol

The HiDiscovery protocol can change the IP address of the Magnum 12KX switch based on the MAC address.

HiDiscovery is a Layer 2 protocol.

Note: For security reasons, restrict the HiDiscovery function for the Magnum 12KX or disable it after the IP parameters have been assigned to the device.

Enabling/disabling the HiDiscovery Function

☐ Select the `Basics:Network` dialog.

☐ Disable the HiDiscovery function in the "HiDiscovery Protocol" frame or limit the access to "read-only".

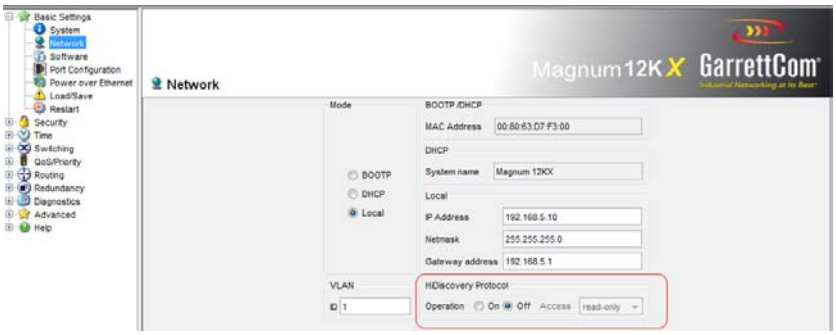


FIGURE 48 – Disabling the HiDiscovery protocol.

`enable`	**Switch to the Privileged EXEC mode.**
`network protocol hidiscovery off`	**Disable HiDiscovery function.**
`network protocol hidiscovery read-only`	**Enable HiDiscovery function with "read-only" access.**
`network protocol hidiscovery read-write`	**Enable HiDiscovery function with "read-write" access.**

FIGURE 49 – Disabling the HiDiscovery protocol using CLI

Port Security

The Magnum 12KX switch can be configured so that every port is protected from unauthorized access. Depending on the selection, the Magnum 12KX checks the MAC address or the IP address of the connected device.

The following functions are available for monitoring every individual port:

- The Magnum 12KX can distinguish between authorized and unauthorized access and supports two types of access control:
  - Access for all:
    – no access restriction.
    – MAC address 00:00:00:00:00:00 or
    – IP address 0.0.0.0.
  - Access exclusively for defined MAC and IP addresses:
    – only devices with defined MAC or IP addresses have access.
    –up to 10 IP addresses, MAC addresses or mask-able MAC addresses can be defined.
- The Magnum 12KX can react to an unauthorized access attempt in 3 selectable ways:
  - none: no response
  - trapOnly: messages by sending a trap. Note - make sure trap stations are defined.
  - portDisable: messages by sending a trap and disabling the port. Note - make sure trap stations are defined.

Example for Port Security

For a LAN connection that is accessible to everyone, set the Magnum 12KX so that only defined users can use the LAN connection. To enable that, activate the port access control on this port. An unauthorized access attempt will cause the Magnum 12KX to shut down the port and alert the user with an alarm message.
The following is known:

Parameter	Value	Explanation
Allowed Addresses	IP 10.0.1.228 10.0.1.229	The defined users are the device with the IP address 10.0.1.228 and the device with the IP address 10.0.1.229
Action	portDisable	Disable the port with the corresponding entry in the port configuration table and send an alarm

Table 5: Port Security Example

Prerequisites for further configuration:

- The port for the LAN connection is enabled and configured correctly
- Prerequisites for the Magnum 12KX to be able to send an alarm (trap)
  - At least one trap recipient under `Diagnostics:Alarms(Traps)`dialog is defined
  - The “Active” column for at least one recipient has been set
  - In the “Selection” frame for trap type, “Port Security” has been selected

Using the Web Interface:

☐ Select the `Security:Port Security` dialog.

☐ In the “Configuration” frame, select “IP-Based Port Security”.

☐ In the table, click on the row of the port to be protected, in the “Allowed IP addresses” cell.
☐ Enter in sequence:
- the IP address: 10.0.1.228
- a space character as a separator
- the IP address: 10.0.1.229

Entry: `10.0.1.228 10.0.1.229`

☐ In the table, click on the row of the port to be protected, in the “Action” cell, and select `portDisable`.

FIGURE 50 – Port Security using IP addresses.

To enter a MAC address select the MAC Based Port Security and modify the MAC address.

Save the settings:

☐ Select the dialog `Basic Settings:Load/Save`.
☐ In the “Save” frame, select “To Device” for the location and click “Save” to permanently save the configuration in the active configuration.

FIGURE 51 – Saving the settings.

Port Authentication using IEEE 802.1X

IEEE 802.1X is also commonly called RADIUS. There are differences in the protocol and implementation details. These nuances are not covered in this section. Both require a "RADIUS" server to authenticate access.

Port authentication using IEEE 802.1X

The port-based network access control is a method described in the standard IEEE 802.1X to protect IEEE 802 networks from unauthorized access. The protocol controls the access to a port by authenticating and authorizing a Magnum 12KX that is connected to this port of the device.

The authentication and authorization is performed by the authenticator, in this case the Magnum 12KX switch. The switch authenticates (or does not authenticate) the supplicant (the querying device, e.g. a PC), which means that it permits the access to the services it provides (e.g. access to the network to which the Magnum 12KX is connected), or else refuses it. In the process, the Magnum 12KX accesses an external authentication server (RADIUS server), which checks the authentication data of the supplicant. The Magnum 12KX exchanges the authentication data with the supplicant via the Extensible Authentication Protocol over LANs (EAPOL), and with the RADIUS server via the RADIUS protocol.

FIGURE 52– RADIUS server connection

Authentication Process according to IEEE 802.1X

A supplicant (usually a PC) attempts to communicate via a device port.

- The Magnum 12KX switch requests authentication from the supplicant. At this time, only EAPOL traffic is allowed between the supplicant and the Magnum 12KX.
- The supplicant replies with its identification data.
- The Magnum 12KX forwards the identification data to the authentication server.
- The authentication server responds to the request in accordance with the access rights.
- The Magnum 12KX evaluates this response and provides the supplicant with access to this port (or leaves the port in the blocked state).

Configuring IEEE 802.1X Port Authentication

The steps needed are:

☐ Configure the user-specific IP parameters (for the Magnum 12KX). Without the proper IP parameters, the switch cannot communicate with the RADIUS server.
☐ Globally enable the 802.1X port authentication function.

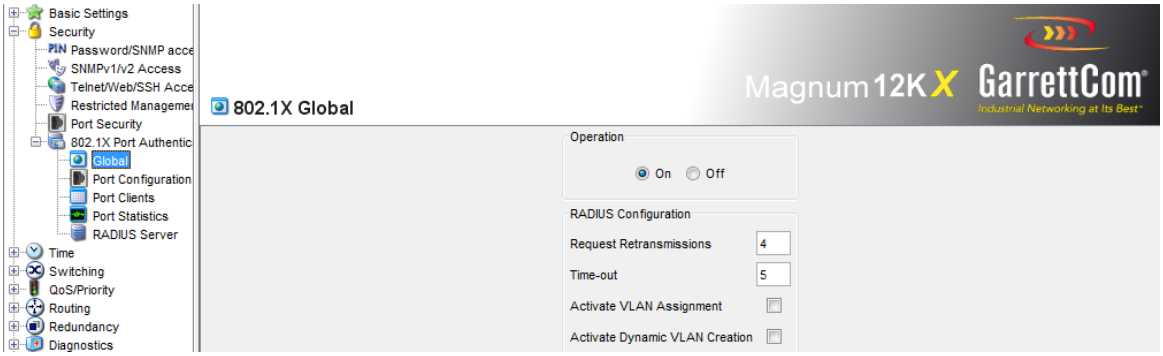
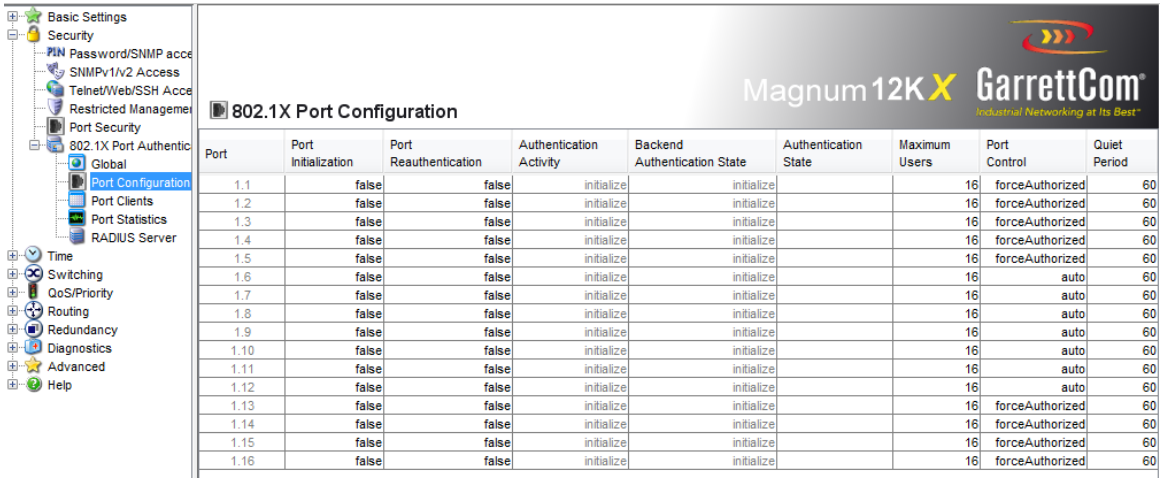


FIGURE 53 – Enabling global 802.1X settings.

Variable	Meaning	Possible values	Default setting
Operation	Switches the function on or off	On, Off	Off
Request Retransmissions	Specify how often the Switch resubmits an unanswered request to the RADIUS server before it sends the request to another RADIUS server.	1 - 15	4
Time-out	Sets how long (in seconds) the Switch waits for a response from the RADIUS server before it resends the request.	1 - 30 s	5 s
Activating the VLAN assignment	Activates or deactivates the assigning of a VLAN ID via the RADIUS server to a port. If a device places a query to a port via 802.1X, the RADIUS server will optionally send along a VLAN ID when a positive response is returned. If this function has been activated, the Switch then incorporates the port as an untagged member in the VLAN specified and sets the port VLAN ID to this value. Note the following information about VLAN assignment.	On, Off	Off

☐ Set the 802.1X Port Control to "auto". The default setting is "force-Authorized".



Port	Port Initialization	Port Reauthentication	Authentication Activity	Backend Authentication State	Authentication State	Maximum Users	Port Control	Quiet Period
1.1	false	false	initialize	initialize		16	forceAuthorized	60
1.2	false	false	initialize	initialize		16	forceAuthorized	60
1.3	false	false	initialize	initialize		16	forceAuthorized	60
1.4	false	false	initialize	initialize		16	forceAuthorized	60
1.5	false	false	initialize	initialize		16	forceAuthorized	60
1.6	false	false	initialize	initialize		16	auto	60
1.7	false	false	initialize	initialize		16	auto	60
1.8	false	false	initialize	initialize		16	auto	60
1.9	false	false	initialize	initialize		16	auto	60
1.10	false	false	initialize	initialize		16	auto	60
1.11	false	false	initialize	initialize		16	auto	60
1.12	false	false	initialize	initialize		16	auto	60
1.13	false	false	initialize	initialize		16	forceAuthorized	60
1.14	false	false	initialize	initialize		16	forceAuthorized	60
1.15	false	false	initialize	initialize		16	forceAuthorized	60
1.16	false	false	initialize	initialize		16	forceAuthorized	60

FIGURE 54 – Enabling global 802.1X for each port.

The table values are as follows:

Variable	Meaning	Possible values	Default setting
Port Initialization	For resetting the initialization function. Setting this attribute to "true" causes the Magnum 12KX to reset the function for this port. When the resetting process is concluded, the value is reset to "false".	true, false	false
Port Reauthentication	Activating and deactivating the reauthentication of the port. Setting this attribute "true" causes the Magnum 12KX to ask the supplicant to reauthenticate itself on this port. The Magnum 12KX resets the value to "false" following a reauthentication.	true, false	false
Authentication Activity	Displays the current status of the authentication activity.	1 = initialize 2 = disconnected 3 = connecting 4 = authenticating 5 = authenticated 6 = aborting authenticating 7 = held 8 = force authorized 9 = force unauthorized	
Server Authentication Status	Displays the current status of the authentication server.	1 = request 2 = response 3 = success 4 = fail 5 = timeout 6 = idle 7 = initialize	
Authentication Status	Displays the current value of the authentication status for the port.	authorized = the connected subscriber has been authenticated unauthorized = the connected subscriber has not been authenticated	
Maximum Number of Users	Maximum number of clients that the Magnum 12KX authenticates on a port at the same time. This parameter is effective if the port control has been set (see below) to macBased.	1 - 16	16
Port Control	Setting for the port access control.	ForceAuthorized: Access is also available for all clients without authentication. ForceUnauthorized: Access is blocked for all clients, even for clients with authentication. auto: Access to the port depends on the result of the authentication. macBased: Access is only available for clients with a MAC address which the client uses in the course of authentication. Note: In the ForceAuthorized, ForceUnauthorized and auto modes the Switch opens or	ForceAuthorized

		blocks the port for all clients. Use these modes if a single client has been connected to the Switch. In the macBased mode the Switch authenticates the clients based on the individual MAC addresses and allows or blocks their data traffic separately. Use this mode if multi-client authentication is needed or the "MAC Authentication Bypass" function.	
Idle Period	Period in seconds in which the authentication process does not expect authentication from the supplicants.	0-65535	60
Transmit Period	Wait period before the Magnum 12KX resends an EAP packet.	1-65535	30
Supplicant Timeout	Excess time in seconds for the communication between the Magnum 12KX and the supplicant.	1-65535	30
Server Timeout	Excess time in seconds for the communication between the Magnum 12KX and the server.	1-65535	30
Maximum Number of Requests	Maximum number of attempted requests to the supplicants before the authentication process terminates.	1-10	2
Assigned VLAN ID	VLAN that the Switch assigned to the port. The port is an untagged member in this VLAN and the port VLAN ID has the same value. Prerequisite: The port control is set to auto. Note: Using the multi-client setting by setting "Port Control" to macBased, take into account: The device-dependent resolution of possible VLAN assignment conflicts for frames received untagged The VLANs assigned, the current values can be found in the "Port Clients" table	0 - 4094	0
Assignment Reason	Reason for assigning the VLANs to the port. Prerequisite: The port control is set to auto. Note: If the multi-client setting by setting is being used"Port Control" to macBased, take into account: The device-dependent resolution of possible VLAN assignment conflicts for frames received untagged. The VLANs assigned, the current values can be found in the "Port Clients" table.	notAssigned, radius, unauthenticatedVLAN	notAssigned

☐ Enter the "shared secret" between the authenticator and the RADIUS server. The shared secret is a text string specified by the RADIUS server administrator.

☐ Enter the IP address and the port of the RADIUS server. The default UDP port of the RADIUS server is port 1812.

Configuration of the RADIUS Server

☐ Select the `Security:802.1x Port Authentication:RADIUS Server` dialog.

This dialog allows the user to enter the data for up to three RADIUS servers.

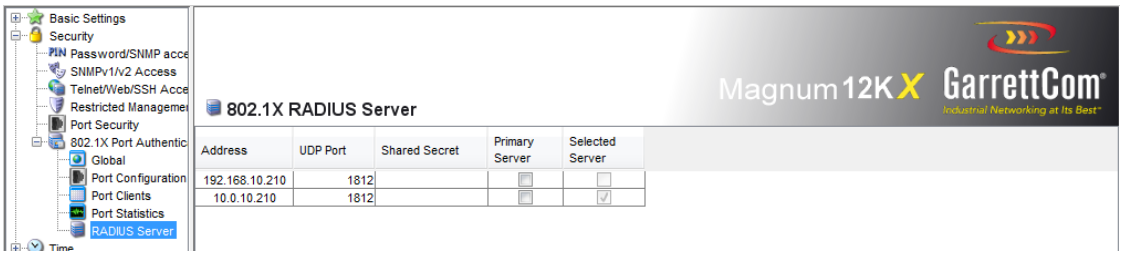


FIGURE 55 – Defining the RADIUS Servers

☐ Click "Create entry" to open the dialog window for entering the IP address of a RADIUS server.
☐ Confirm the IP address entered using "OK". Create a new row in the table for each RADIUS server.
☐ In the "Shared Secret" column enter the character string representing the key provided by the administrator of the RADIUS server.
☐ With "Primary Server" name this server as the first server which the Magnum 12KX should contact for port authentication queries. If this server is not available, the Magnum 12KX contacts the next server in the table.
☐ "Selected server" shows which server the Magnum 12KX actually sends its queries to.
☐ With "Delete entry" delete the selected row in the table.

Selecting Ports

☐ Select the `Security:802.1x Port Authentication:Port Configuration` dialog.
☐ In the "Port control" column select "auto" for the ports for which need to be activated the port-related network access control. This has been discussed earlier in this section.

Activating Access Control (RADIUS)

☐ Select the `Security:802.1x Port Authentication:Global` dialog.
☐ With "Function" Enable RADIUS. The same interface is used for disabling RADIUS.

Access Control Lists (ACL)

Use Access Control Lists (ACL) to filter out, forward, divert or prioritize data packets as they are received. The Magnum 12KX provides

- MAC-based ACLs and
- IP-based ACLs.

The Magnum 12KX executes the directives set by the ACLs when it receives a packet. This is why the lists are called Ingress ACLs.

The Magnum 12KX provides the following ACL capabilities:

- Up to 100 ACLs
- 10 rules per ACL
- Up to 100 rules per interface
- Up to 1000 rules on all interfaces combined
- Possible actions:
  - permit and deny
  - in combination with permit: assign queue and redirect i.e. if a rule applies, the packet is forwarded to the specific interface.
- "Deny everything" is always the (invisible) final rule. It comes into effect if no other rules apply to this interface.

The configuration of ACLs consists of the following steps:

☐ First define ACL and then
☐ Assign the ACLs to all physical ports and to all link aggregation interfaces.

The sequence used in defining the rules of a list and the sequence in which these lists are connected to an interface determines the sequence in which the rules and lists are.

Prioritizing with ACLs

Prioritizing with ACLs provides an extension of the prioritizing function. Using the "assign queue" ACL action, one can perform extended prioritizing using protocols, source and destination addresses, VLAN ID, and so on.

If an ACL rule containing an assign queue action applies to a packet received, the Magnum 12KX modifies the priority information in the data packet in accordance with the specified assign queue parameter. This procedure is known as ACL remarking. The Magnum 12KX sends the data packets with the modified priority information.

Assign queue parameter	VLAN priority	DSCP
0	0	CS0 (0)
1	1	CS1 (8)
2	2	CS2 (16)
3	3	CS3 (24)
4	4	CS4 (32)
5	5	CS5 (40)
6	6	CS6 (48)
7	7	CS7 (56)

Table 6: Assigning the assign queue parameters to the modified VLAN priority and to the modified DSCP value.

IP-based ACLs

The Magnum 12KX differentiates between standard and extended IP-based ACLs. ACLs with an ID number (ACL ID)

- 1 to 99 are standard IP-based ACLs and
- 100 to 199 are extended IP-based ACLs.

Standard IP-based ACLs provide the following criteria for filtering:

- IP source address with network mask
- All data packets (match every)

Extended IP-based ACLs provide the following criteria for filtering:

- All data packets (every)
- Protocol number or protocol (IP, ICMP, IGMP, TCP, UDP)
- IP source address with network mask or all IP source addresses (any)
- Layer 4 protocol port numbers of the source (UDP port, TCP port)
- IP destination address with network mask or all IP destination addresses (any)
- Layer 4 protocol port numbers of the destination (UDP port, TCP port)
- ToS field with mask
- DSCP field
- IP precedence field

Note: IP address masks in the rules of ACLs are inverse.
This means that if a single IP address needs to be masked, the network mask 0.0.0.0 needs to be selected.

MAC-based ACLs

While an ID number is used to identify IP-based ACLs, a unique needs to be used to identify MAC-based ACLs. MAC based ACLs have a number between 1 and 99.

MAC-based ACLs provide the following criteria for filtering:

- Source MAC address with masks or all sources (any)
- Destination MAC address or all destinations (any)
- Ethernet type

- VLAN ID
- VLAN priority (COS)
- Secondary VLAN ID
- Secondary VLAN priority

Note: If using MAC ACLs at ports located in the MRP-Ring, add the following rule to the ACLs:

- PERMIT
- Source MAC: ANY
- Destination MAC: 01:15:4E:00:00:00
- Destination MAC mask: 00:00:00:00:00:03
- CLI command in the Config-mac-access mode:
  `permit any 01:15:4E:00:00:00 00:00:00:00:00:03`

Note: MAC address masks in the rules of ACLs are inverse.
This means that if a single MAC address needs to be masked, select the network mask 00:00:00:00:00:00.

If MAC addresses in the range from 00:80:63:00:00:00 to 00:80:63:FF:FF:FF needs to be masked, select the network mask 00:00:00:FF:FF:FF.

Configuring IP ACLs

Example: Extended ACL

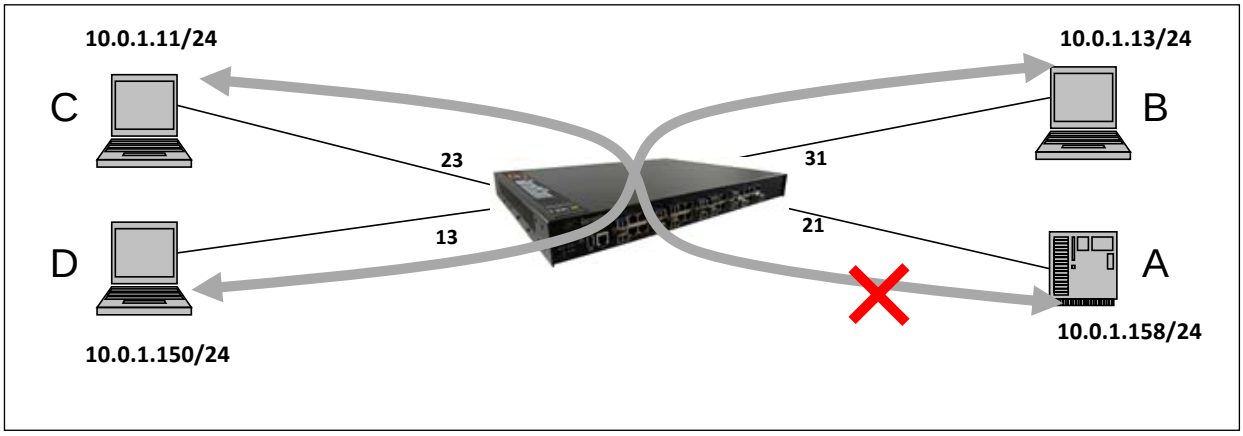


FIGURE 56 – ACL example.

B and C are not allowed to communicate with A.

`enable`	**Switch to the Privileged EXEC mode.**
`configure`	**Switch to the Configuration mode.**
`access-list 100 deny ip 10.0.1.11 0.0.0.0 10.0.1.158 0.0.0.0`	**Create the extended ACL 100 with the first rule. This denies data traffic from IP source address 10.0.1.11 to the IP destination address 10.0.1.158.**
`access-list 100 permit ip any any`	**Add another rule to the ACL 100. This permits data traffic from any IP source address to any IP destination address.**

```
access-list 110 deny ip 10.0.1.13 0.0.0.0 10.0.1.158 0.0.0.0
```
Create the extended ACL 110 with the first rule. This denies data traffic from IP source address 10.0.1.13 to the IP destination address 10.0.1.158.

```
access-list 110 permit ip any any
```
Add another rule to the ACL 110. This permits data traffic from any IP source address to any IP destination address.

```
exit
```
Switch to the privileged EXEC mode.

```
show ip access-lists 100
```
Displays the rules of ACL 100.

```
ACL ID: 100


Rule Number: 1
Action..................................... deny
Match All.................................. FALSE
Protocol................................... 255(ip)
Source IP Address.......................... 10.0.1.11
Source IP Mask............................. 0.0.0.0
Destination IP Address..................... 10.0.1.158
Destination IP Mask........................ 0.0.0.0

Rule Number: 2
Action..................................... permit
Match All.................................. TRUE
```

```
configure
```
Switch to the Configuration mode.

```
interface 2/3
```
Switch to the Interface Configuration mode of -interface 2.3.

```
ip access-group 100 in
```
Attaches ACL 100 to interface 2.3 for received data.

```
exit
```
Switch to the Configuration mode.

```
interface 3/1
```
Switch to the interface configuration mode of interface 3.1.

```
ip access-group 110 in
```
Attaches ACL 110 to interface 3.1 for received data.

```
exit
```
Switch to the Configuration mode.

```
exit
```
Switch to the privileged EXEC mode.

```
show access-lists interface 2/3 in

ACL Type             ACL ID              Sequence Number
-------- ------------------------------ ---------------
IP       100                            1
```

FIGURE 57 – Configuring ACLs.

Configuring MAC ACLs

Example: MAC ACL
Filtering AppleTalk and IPX from the entire network.

```
enable                          Switch to the Privileged EXEC mode.
configure                       Switch to the Configuration mode.
mac access-list                 Create the extended ACL "ipx-apple".
extended ipx-apple
deny any any ipx                Add the rule "deny IPX" to the list.
deny any any appletalk          Add the rule "deny AppleTalk" to the list.
                                Add the rule "permit all other data" to the list.
permit any any
exit                            Switch to the Configuration mode.


mac access-group                Attach the ACL "ipx-apple" to all interfaces.
ipx-apple in
exit                            Switch to the privileged EXEC mode.


show mac access-lists           Display the ACLs.
     MAC ACL Name               Rules Direction      Interface(s)
------------------------------- ----- --------- ------------------
ipx-apple                       3     inbound   1/1,1/2,1/3,1/4...


show      access-lists          Display the ACLs of interface 1.1.
interface 1/1 in
ACL Type             ACL ID              Sequence Number
-------- ------------------------------- ---------------
MAC      ipx-apple                       1
```

FIGURE 58 – MAC ACL example

Configuring Priorities with IP ACLs

Example: Prioritizing Multicast streams.

- Assign priority 6 to the Multicast streams with the IP Multicast destination addresses 239.1.1.1 to 239.1.1.255 and
- Assign priority 5 to the Multicast streams with the IP Multicast destination addresses 237.1.1.1 to 237.1.1.255 and

```
enable                  Switch to the Privileged EXEC mode.
configure               Switch to the Configuration mode.
```

```
access-list 102 permit ip any 239.1.1.1 0.0.0.255 -assign-queue 6
```
Create the extended ACL 102 with the first rule. This rule assigns priority 6 to the IP Multicast destination addresses 239.1.1.1 with the mask 0.0.0.255.

```
access-list 102 permit ip any 237.1.1.1 0.0.0.255 -assign-queue 5
```
Add another rule to the ACL 102. This rule assigns priority 5 to the IP Multicast destination addresses 237.1.1.1 with the mask 0.0.0.255.

```
exit
```
Switch to the privileged EXEC mode.

```
show ip access-lists 102
```
Displays the rules of ACL 102.

```
ACL ID: 102

Rule Number: 1
Action..................................... permit
Match All.................................. FALSE
Protocol................................... 255(ip)
Destination IP Address..................... 239.1.1.1
Destination IP Mask........................ 0.0.0.255
Assign Queue............................... 6

Rule Number: 2
Action..................................... permit
Match All.................................. FALSE
Protocol................................... 255(ip)
Destination IP Address..................... 237.1.1.1
Destination IP Mask........................ 0.0.0.255
Assign Queue............................... 5
```

FIGURE 59 – Setting priorities with ACL.

Example: Extended ACL with prioritizing using the Simple Network Management Protocol (SNMP, Layer 4)

```
enable
```
Switch to the Privileged EXEC mode.

```
configure
```
Switch to the Configuration mode.

```
access-list 104 permit udp any any eq snmp assign -queue 5
```
Create the extended ACL 104 with the first rule.
This rule assigns priority 5 to all SNMP packets with the UDP destination port (=161).
This rule overwrites any priority contained in a VLAN tag with the value 5, and also overwrites the IP-DSCP value with cs5.

```
exit
```
Switch to the privileged EXEC mode.

```
show ip access-lists 104
```
Displays the rules of ACL 104.

```
ACL ID: 104


Rule Number: 1
Action.....................................
permit
Match All..................................... FALSE
Protocol.....................................
17(udp)
Destination   L4   Port   Keyword..................
161(snmp)
Assign Queue.................................. 5
```

`configure`	**Switch to the Configuration mode.**
`interface 2/1`	**Switch to the Interface Configuration mode of -interface 2.1.**
`ip access-group 104 in`	**Attaches ACL 104 to interface 2.1.**
`exit`	**Switch to the Configuration mode.**
`exit`	**Switch to the privileged EXEC mode.**
`show access-lists interface 2/1 in`	**Display the ACLs attached to interface 2.1 for received data packets.**

```
ACL Type             ACL ID              Sequence Number
-------- ------------------------------- ---------------
IP       100                             1
IP       102                             3
IP       104                             4
```

FIGURE 60 – Extended ACL example.

ACL 100 contains the rule "permit all" at the end. Thus the ACLs 102 and 104 are never applied. Use the sequence number to influence the sequence for processing the ACLs.

Specifying the Sequence of the Rules

The sequence of the ACLs determines their usage. The first list that applies is used, and all subsequent rules are ignored. The sequence can be influenced by assigning the sequence number. A small sequence number has precedence over a higher one.

`enable`	**Switch to the Privileged EXEC mode.**
`configure`	**Switch to the Configuration mode.**
`ip access-group 100 in 30`	**Assign sequence number 30 to ACL 100.**
`ip access-group 102 in 10`	**Assign sequence number 10 to ACL 102.**
`ip access-group 104 in 20`	**Assign sequence number 20 to ACL 104.**
`exit`	**Switch to the privileged EXEC mode.**

```
show access-lists
interface 2/1 in
```

Display the ACLs attached to interface 2.1 for received data packets.

```
ACL Type             ACL ID                          Sequence Number
-------- ------------------------------- ---------------
IP       100                             30
IP       104                             20
IP       102                             10
```

FIGURE 61 – Specifying sequence numbers for ACLs.

Finally after completing all the configuration work, do not forget to save the changes.

Chapter 7

Synchronizing System Time

Magnum 12KX provides two options with different levels of accuracy for synchronizing the time in the network.

If the accuracy required is in the order of milliseconds, the Simple Network Time Protocol (SNTP) provides the solution needed. The accuracy depends on the proximity of the startum clock from which the timing information is synchronized and other network parameters.

IEEE 1588 with the Precision Time Protocol (PTP) achieves accuracies in the order of fractions of microseconds. This superior method is suitable for process control, power sub-stations and other situations where a small error in timing accuracy can cause potential damage or losses.

Examples where precise timing is needed include:
- log entries – to make sense as to when the event occurred
- time stamping of production data
- production control, etc.

Select the method (SNMP or PTP) that best suits the user requirements. Both methods can be used simultaneously since they interact.

Entering the Time

If no reference clock is available, the system time can be set manually.

Note that once the time is set (either manually or through another statum clock or a grandmaster clock), the 12KX can then be used as a reference clock.

Note: When setting the time in zones with summer and winter times, make an adjustment for the local offset.

Note: Magnum 12KX can also get the SNTP server IP address and the local offset from a DHCP server.

Setting the time manually:

☐ Select the `Time` dialog.
☐ Using a Web browser, the Magnum 12KX switch synchronizes the time from the local PC. It is recommended that the PC clock be synchronized first before the Magnum 12KX time is set.

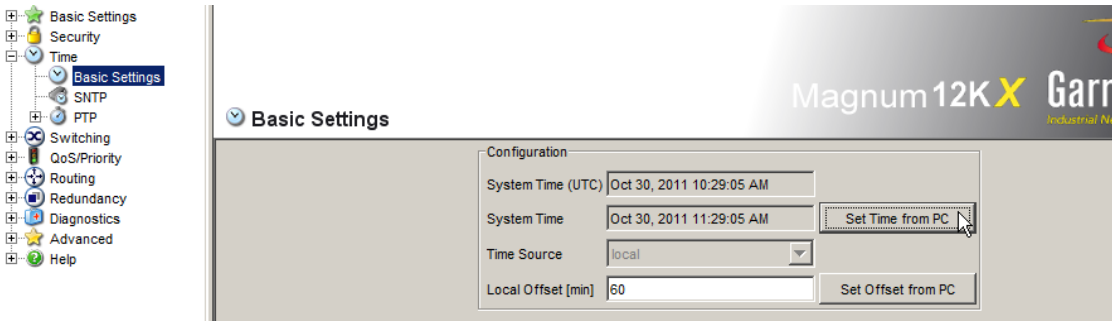


FIGURE 62 – Setting the system time. Note the time is set from the local PC. To define an offset, use the "Set Offset" button.

With the `Time` dialog time-related settings can be changed independently of the time synchronization protocol selected.

- The "IEEE 1588 time" displays the time determined using PTP.
  The "SNTP time" displays the time with reference to Universal Time Coordinated (UTC).
  The display is the same worldwide. Local time differences are not taken into account.
- The "System time" uses the "IEEE 1588 / SNTP time", allowing for the local time difference from "IEEE 1588 / SNTP time".
  "System time" = "IEEE 1588 / SNTP time" + "Local offset".
- "Time source" displays the source of the following time data. The Magnum 12KX automatically selects the source with the greatest accuracy.
  Possible sources are: `local` and `sntp`. The source is initially `local`. If SNTP is activated and if the Magnum 12KX receives a valid SNTP packet, it sets its time source to `sntp`.

☐ With "Set time from PC", the Magnum 12KX takes the PC time as the system time and calculates the IEEE 1588 / SNTP time using the local time difference.
"IEEE 1588 / SNTP time" = "System time" - "Local offset"

☐ The "Local Offset" is for displaying/entering the time difference between the local time and the "IEEE 1588 / SNTP time".

With "Set offset from PC", the agent determines the time zone on the PC and uses it to calculate the local time difference.

Setting the time manually using CLI:

`enable`	**Switch to the Privileged EXEC mode.**
`configure`	**Switch to the Configuration mode.**
`sntp time <YYYY-MM-DD HH:MM:SS>`	**Set the system time of the Magnum 12KX.**
`sntp client offset <-1000 to 1000>`	**Enter the time difference between the local time and the "IEEE 1588 / SNTP time".**

FIGURE 63 – Setting time using CLI.

SNTP

SNTP or Simple Network Time Protocol is commonly used in TCP/IP networks to synchronize time.

Description of SNTP

The Simple Network Time Protocol (SNTP) enables the user to synchronize the system time in the network.

The Magnum 12KX supports the SNTP client and the SNTP server function.

The standard timescale used by most nations of the world is Coordinated Universal Time (UTC), which is based on the Earth's rotation about its axis. Time Zone offsets are typically set to the UTC, including GMT, which is an approximation of UTC.

International Atomic Time (TAI, from the French name Temps Atomique International) is a high-precision atomic time standard that tracks proper time on Earth's period. TAI is the principal realization of Terrestrial Time, and the basis for Coordinated Universal Time (UTC) which is used for civil timekeeping all over the Earth's surface. The Gregorian calendar, which is based on the Earth's rotation about the Sun, uses the UTC to designate things such as time, date, month, year etc. The UTC timescale is modified with respect to International Atomic Time or Temps Atomique International (TAI) by inserting leap seconds at intervals of about 18 months. UTC time is disseminated by various means, including radio and satellite navigation systems, telephone modems and portable clocks.

In 1981 the time synchronization technology was documented in the now historic Internet Engineering Note series as IEN-173. The first specification of a public protocol developed from it appeared in RFC-778. The first deployment of the technology in a local network was as an integral function of the Hello routing protocol documented in RFC-891, which survived for many years in a network prototyping and test bed operating system called the Fuzzball. There was considerable discussion during 1989 about the newly announced Digital Time Synchronization Service (DTSS), which was adopted for the Enterprise network. The DTSS and NTP communities had much the same goals, but somewhat different strategies for achieving them. One problem with DTSS, as viewed by the NTP community, was a possibly serious loss of accuracy, since the DTSS design did not discipline the clock frequency. The problem with the NTP design, as viewed from the DTSS community, was the lack of formal correctness principles in the design process.

Simple Network Protocol (SNTP) is described in RFC-1769 as well as in RFC-2030. SNTP is compatible with NTP as implemented for the IPv4, IPv6 and OSI protocol stacks. SNTP has been used in several standalone NTP servers integrated with GPS receivers.

The article from NIST http://tf.nist.gov/timefreq/service/pdf/computertime.pdf provides details on time synchronization services as well as ports time synchronization services need to communicate on. http://physics.nist.gov/GenInt/Time/time.html provides a walk through the history of time and time synchronization on the NIST site. There are many other interesting articles available on Internet.

Stratum clocks

NTP uses a hierarchical system of "clock strata". The stratum levels define the distance from the reference clock and exist to prevent cycles in the hierarchy. (Note that this is different from the notion of clock strata used in telecommunications systems.)

Stratum 0

These are devices such as atomic (cesium, rubidium) clocks, GPS clocks or other radio clocks. Stratum-0 devices are not attached to the network; instead they are locally connected to computers (e.g. via an RS-232 connection.) The atomic clock at the NIST Denver facility is an example of the Stratum 0 clock.

Stratum 1

These are computers attached to Stratum 0 devices. Normally they act as time servers for timing requests from Stratum 2 servers via NTP. These computers are also referred to as time servers. Time servers from NIST and USNO are examples of Stratum 1 servers.

Stratum 2

These are computers that send NTP requests to Stratum 1 servers. Normally a Stratum 2 computer will reference a number of Stratum 1 servers and use the NTP algorithm to gather the best data sample, dropping any Stratum 1 servers that seem obviously wrong. Stratum 2 devices will peer with other Stratum 2 devices to provide more stable and robust time for all devices in the peer group. Stratum 2 devices normally act as servers for Stratum 3 NTP requests.

Stratum 3

These devices employ exactly the same NTP functions of peering and data sampling as Stratum 2, and can themselves act as servers for lower strata, potentially up to 16 levels. NTP (depending on what version of NTP protocol in use) supports up to 256 strata.

This is summarized in the figure below.

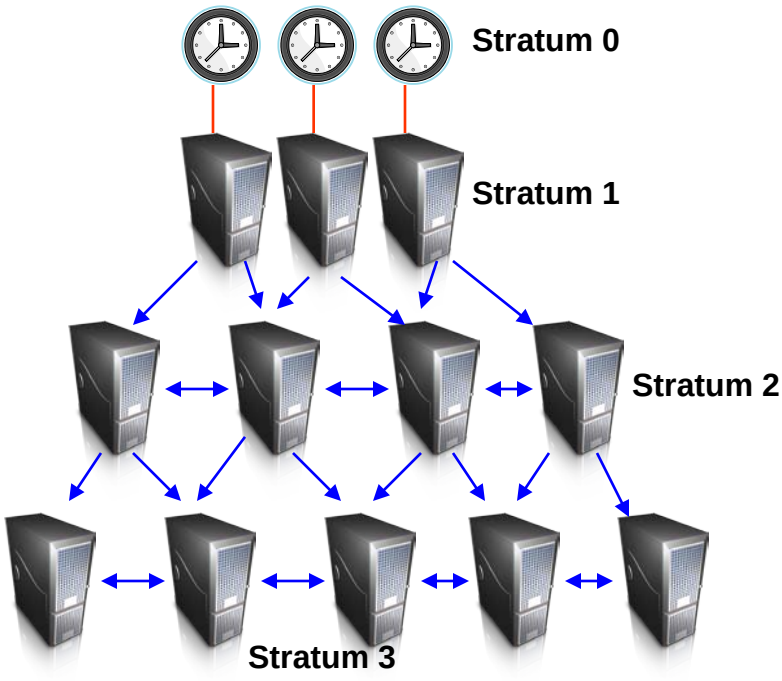


FIGURE 64 – Different Stratum NTP servers

Special purpose receivers are available for many time-dissemination services, including the Global Position System (GPS) and other services operated by various national governments. For reasons of cost and convenience, it is not possible to equip every computer with one of these receivers. However, it is possible to equip some number of computers, routers or switches acting as primary time servers to synchronize a much larger number of secondary servers and clients connected by a common network.

Preparing for SNTP

☐ In a network, define a clock from which other clocks can synchronize their times from. This clock is usually the “grandmaster” or main time source for the TCP/IP network. It is usually a good idea to define a backup time source in case the master clock fails.

☐ Determine how often the clock updates itself from the source.

☐ Define where the source is i.e. how will the master get the source of timing information from. This can be done by synchronizing with a publicly available time source (such as those from www.ntp.org) or by installing a local clock which can synchronize its time from the satellite or GPS or other sources.

☐ For all other devices determine how often they update their time, as well as which are the primary and secondary clock sources.

☐ Enable the SNTP function on all devices whose time needs to be set using SNTP.
The SNTP server of the device responds to Unicast requests as soon as it is enabled.

☐ If no reference clock is available, specify a device as the reference clock and set its system time as accurately as possible.

Configuring SNTP

☐ Select the `Time:SNTP` dialog.

▶ Operation

☐ In this frame SNTP function can be switched on/off.

▶ SNTP Status

☐ The “Status message” displays statuses of the SNTP client as one or more test messages. Possible messages are:
`Local system clock is synchronized; An SNTP loop has occurred; General error; Synchronized one time; Client deactivated; Server 1 is not synchronized; Server 1 has incorrect protocol version; Server 1 not responding; Server 2 is not synchronized; Server 2 has incorrect protocol version; Server 2 not responding`.

▶ Configuration SNTP Client

☐ In “Client status” switch the SNTP client of the Magnum 12KX on/off.

☐ In “External server address” enter the IP address of the SNTP server from which the Magnum 12KX periodically requests the system time.

☐ In “Redundant server address” enter the IP address of the SNTP server from which the Magnum 12KX periodically requests the system time, if it does not receive a response to a request from the “External server address” within 1 second.

Note: If receiving the system time from an external/redundant server address, do not accept any SNTP Broadcasts (see below). This ensures that the Magnum 12KX uses the time of the server entered.

☐ In “Server request interval” specify the interval at which the Magnum 12KX requests SNTP packets (valid entries: 1 s to 3600 s, by default: 30 s).

☐ With “Accept SNTP Broadcasts” the Magnum 12KX takes the system time from SNTP Broadcast/Multicast packets that it receives.

☐ With “Deactivate client after synchronization”, the Magnum 12KX only synchronizes its system time with the SNTP server one time after the client status is activated, then it switches the client off.

Note: If PTP is enabled at the same time, the SNTP client first collects 60 time stamps before it deactivates itself. The Magnum 12KX thus determines the drift compensation for its PTP clock. With the preset server request interval, this takes about half an hour.

- Configuration SNTP Server
  - ☐ In “Server status” switch the SNTP server of the Magnum 12KX on/off.
  - ☐ In “Anycast destination address” enter the IP address to which the SNTP server of the Magnum 12KX sends its SNTP packets.
  - ☐ In “VLAN ID” specify the VLAN to which the Magnum 12KX periodically sends its SNTP packets.
  - ☐ In “Anycast send interval” specify the interval at which the Magnum 12KX sends SNTP packets (valid entries: 1 s to 3,600 s, by default: 120 s).
  - ☐ With “Disable Server at local time source” the Magnum 12KX disables the SNTP server function if the source of the time is `local` (see `Time` dialog).

IP destination address	Send SNTP packet to
0.0.0.0	Nobody
Unicast address (0.0.0.1 - 223.255.255.254)	Unicast address
Multicast address (224.0.0.0 - 239.255.255.254), especially 224.0.1.1 (NTP address)	Multicast address
255.255.255.255	Broadcast address

Table 7: Destination address classes for SNTP packets

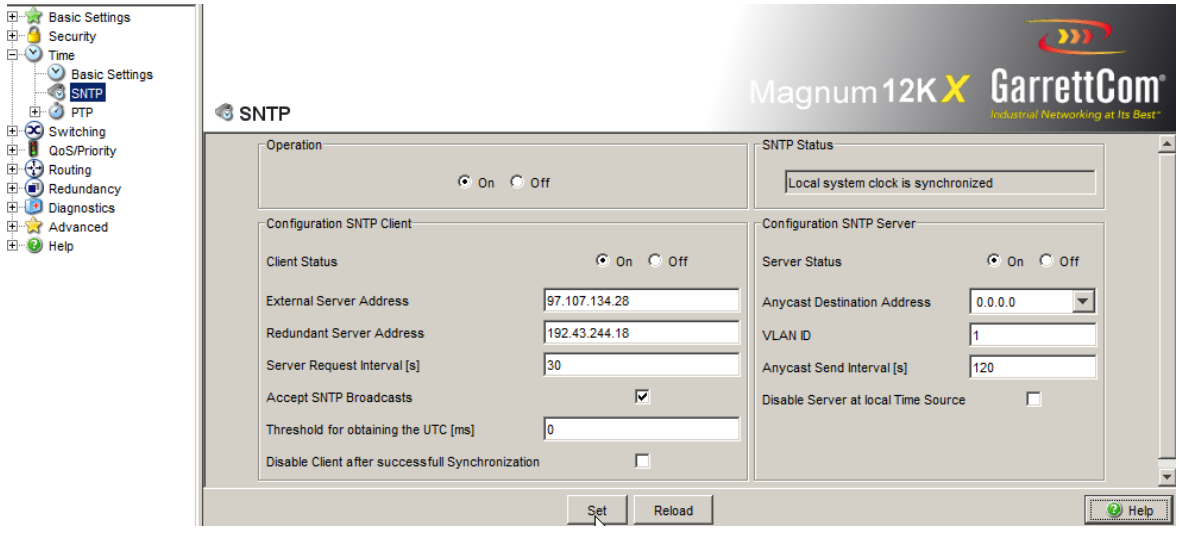


FIGURE 65 – Configuring SNTP.

Device	192.168.1.1	192.168.1.2	192.168.1.3
Operation	On	On	On
Server destination address	0.0.0.0	0.0.0.0	0.0.0.0
Server VLAN ID	1	1	1
Send interval	120	120	120
Client external server address	192.168.1.0	192.168.1.1	192.168.1.2
Request interval	30	30	30
Accept Broadcasts	No	No	No

Table 8: SNTP Settings for the example.

Precision Time Protocol

While SNTP is sufficient for security activities such as SYSLOG, intrusion detection, and others, the accuracy of timing synchronization using SNTP is not sufficient for Smart Grid Applications. For example, a 41 nanosecond difference amounts to one degree offset between two sources of power. The offset causes an increase in “virtual” power, which ultimately translates to revenues which are lost as “wasted” energy. This is especially critical today with different power sources. Power sources vary – power can be generated using coal, natural gas, or other fossil fuels. Power can also be generated from natural occurring energy sources such as sun, wind, tides, geo-thermals etc. These power sources are generally termed as renewable sources or green energy (as they typically do not emit CO_2.) However, these renewable sources are not as consistent as fossil fuel.

The Precision Time Protocol (PTP) is a high-precision time protocol for synchronization used in measurement and control systems which reside on a local area network. Using PTP, accuracy in the sub-microsecond range may be achieved with low-cost implementations. PTP was originally defined in the IEEE 1588-2002 standard, officially entitled "Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems". In 2008 a revised standard, IEEE 1588-2008, was released. This new version, also known as PTP Version 2, improves accuracy, precision, and robustness but Version 2 is not backwards compatible with the original 2002 version (called Version 1). IEEE 1588 is designed to fill a niche not well served by either of the two dominant protocols: NTP and GPS. IEEE 1588 is designed for local systems requiring accuracies beyond those attainable using NTP. It is also designed for applications that cannot bear the cost of a GPS receiver at each node, or when GPS signals are inaccessible.

Architecture - The IEEE 1588 standards describe hierarchical master-slave architecture for clock distribution. Under this architecture, a time distribution system consists of one or more communication mediums (network segments), and one or more clocks.

The **ordinary clock** is a device with a single network connection and is either the source of (master) or destination for (slave) synchronization reference.

The **boundary clock** has multiple network connections and can accurately bridge synchronization from one network segment to another.

A **synchronization master** is elected for each of the network segments in the system. The root timing reference is called the **grandmaster**. The grandmaster transmits synchronization information to the clocks residing on its network segment. The boundary clocks with a presence on that segment then relay accurate time to the other segments to which they are connected.

A simplified PTP system frequently consists of ordinary clocks connected to a single network. No boundary clocks are used. A grandmaster is elected and all other clocks synchronize directly to it.

IEEE 1588-2008 introduces a clock associated with network equipment used to convey PTP messages. The transparent clock modifies PTP messages as they pass through the Magnum 12KX. Timestamps in the messages are corrected for time spent traversing the network equipment. This scheme improves distribution accuracy by compensating for delivery variability across the network.

Some salient features of IEEE 1588 protocol can be summarized as:

- International standard
- Timing synchronization can be implemented over packet based networks e.g. Ethernet
- High accuracy – sub microsecond synchronization
- Simple – can be implemented in hardware or software
- Minimal overhead – network, processor, management
- Protocol – can be implemented on different networks

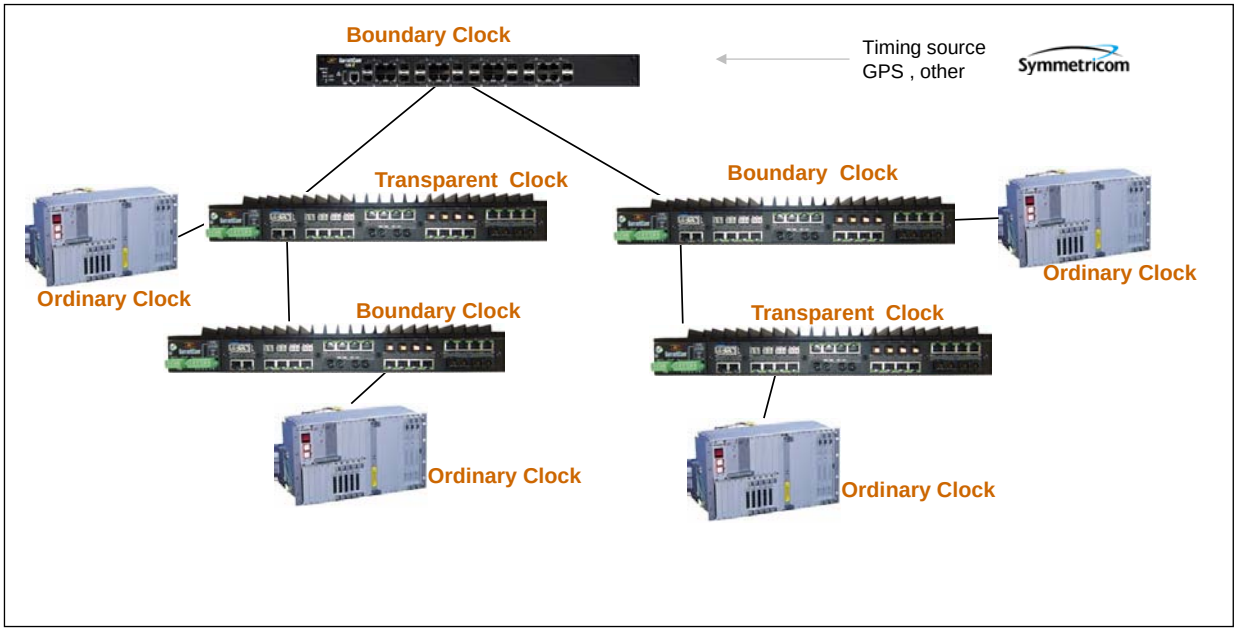


FIGURE 66 – Example of a PTP network using Magnum 12KX and Magnum 10KT along with Industrial SCADA equipment.

IEEE 1588 is implemented as a message-based protocol. For example, event messages such as s*ync*, *delay-request*, *follow up*, *delay response* are used by ordinary clocks and boundary clocks to synchronize timing information. Similarly event messages are used by *transparent clocks* to measure and compensate for delays.

General messages are used for non-critical timing functions. For example, signaling messages are used for non-critical information and Announce messages are used to develop a clock hierarchy. Management messages are used to configure and manage PTP.

All PTP messages are sent using multicast messaging. IEEE 1588-2008 introduces an option for devices to negotiate unicast transmission on a port-by-port basis. PTP messages may use the Internet Protocol (IP) for transport. The original specification used only IPv4 transports, but this has been extended to IPv6. Over IP, messages use the User Datagram Protocol (UDP). Datagrams are transmitted using IP multicast addressing, for which multicast group addresses are defined for IPv4 and IPv6. Event messages are sent to port number 319. General messages use port number 320. Replies to Management messages are always returned to the unicast address of the originator. The messages used by PTP are multicast messages. Encapsulation is also defined for bare IEEE 802.3 Ethernet, DeviceNet, ControlNet and PROFIBUS. PTP uses Ethertype 0x88F7 and an Ethernet multicast destination address of 01-1B-19-00-00-00 for all but peer delay messages. Peer delay messages are sent to 01-80-C2-00-00-0E.

Description of PTP Functions

Precise time management is required for running time-critical applications via a LAN.
The IEEE 1588 standard with the Precision Time Protocol (PTP) describes a procedure that assumes one clock is the most accurate and thus enables precise synchronization of all clocks in a LAN.

This procedure enables the synchronization of the clocks involved to an accuracy of a few 100 ns. The synchronization messages have virtually no effect on the network load. PTP uses Multicast communication.

Factors influencing precision are:

- Accuracy of the reference clock
  IEEE 1588 classifies clocks according to their accuracy. An algorithm that measures the accuracy of the clocks available in the network specifies the most accurate clock as the "Grandmaster" clock.

PTPv1 Stratum -number	**PTPv2 Clock class**	**Specification**
0	(priority 1 = 0)	For temporary, special purposes, in order to assign a higher accuracy to one clock than to all other clocks in the network.
1	6	Indicates the reference clock with the highest degree of accuracy. The clock can be both a boundary clock and an ordinary clock. Stratum 1/ clock class 6 clocks include GPS clocks and calibrated atomic clocks. A stratum 1 clock cannot be synchronized using the PTP from another clock in the PTP system.
2	6	Indicates the second-choice reference clock.
3	187	Indicates the reference clock that can be synchronized via an external connection.
4	248	Indicates the reference clock that cannot be synchronized via an external connection. This is the standard setting for boundary clocks.
5–254	–	Reserved.
255	255	Such a clock should never be used as the best master clock.

Table 9: Stratum classification of the clocks.

- Cable delays; device delays:
  The communication protocol specified by IEEE 1588 enables delays to be determined. Formulas for calculating the current time eliminate delays.
- Accuracy of local clocks:
  The communication protocol specified by IEEE 1588 takes into account the inaccuracy of local clocks in relation to the reference clock. Calculation formulas permit the synchronization of the local time, taking into account the inaccuracy of the local clock in relation to the reference clock.

  To get around the delay and jitter in the protocol stack, IEEE 1588 recommends inserting a special hardware time stamp unit between the MAC and Physical layers.

  The delay and jitter in the LAN increase in the media and transmission devices along the transmission path.

  With the introduction of PTP version 2, two procedures are available for the delay measurement:
- End-to-End (E2E):
  E2E corresponds to the procedure used by PTP version 1. Every slave clock measures only the delay to its master clock.
- Peer-to-Peer (P2P):
  With P2P, like in E2E, every slave clock measures the delay to its master clock. In addition, in P2P every master clock measures the delay to the slave clock. For example, if a redundant ring is interrupted, the slave clock can become the master clock and the master clock can become the slave clock. This switch in the synchronization direction takes place without any loss of precision, as with P2P the delay in the other direction is already known.

The cable delays are relatively constant. Changes occur very slowly. IEEE 1588 takes this fact into account by regularly making measurements and compensating calculations.

IEEE 1588 eliminates the inaccuracy caused by delays and jitter by defining boundary clocks. Boundary clocks are clocks integrated into devices. These clocks are synchronized on the one side of the signal path, and on the other side of the signal path they are used to synchronize the subsequent clocks (ordinary clocks).
PTP version 2 also defines what are known as transparent clocks. A transparent clock cannot itself be a reference clock, nor can it synchronize itself with a reference clock. However, it corrects the PTP messages it transmits by its own delay time and thus removes the jitter caused by the transmission. When cascading multiple clocks in particular, transparent clocks can be used to achieve greater time precision for the connected terminal devices than with boundary clocks

Independent of the physical communication paths, the PTP provides logical communication paths which are defined by setting up PTP subdomains. Subdomains are used to form groups of clocks that are time-independent from the rest of the domain. Typically, the clocks in a group use the same communication paths as other clocks.

Configuring PTP

After PTP function is activated, the switch software manages the PTP configuration automatically. The default settings of the Magnum 12KX are sufficient for most network situations. The steps below highlight the planning needed to implement PTP.

☐ To get an overview of the time distribution, draw a network plan with all the devices participating in PTP.

Note: Connect all the connections needed to distribute the PTP information to connections with an integrated time stamp unit (RT modules).

Note: Devices without a time stamp unit take the information from the PTP and use it to set their clocks. They are not involved in the protocol.

☐ Enable the PTP function on all devices whose time need synchronizing using PTP.

☐ Select the PTP version and the PTP mode. Select the same PTP version for all the devices that need synchronizing.

PTP mode	Application
v1-simple-mode	Support for PTPv1 without special hardware. The Magnum 12KX synchronizes itself with received PTPv1 messages. Select this mode for devices without a timestamp unit (RT module).
v1-boundary-clock	Boundary Clock function based on IEEE 1588-2002 (PTPv1).
v2-boundary-clock-onestep	Boundary Clock function based on IEEE 1588-2008 (PTPv2) for devices with MM23 and MM33 media modules. The one-step mode determines the precise PTP time with one message.
v2-boundary-clock-twostep	Boundary Clock function based on IEEE 1588-2008 (PTPv2) for devices with RT modules. The two-step mode determines the precise PTP time with two messages.
v2-simple-mode	Support for PTPv2 without special hardware. The Magnum 12KX synchronizes itself with received PTPv2 messages. Select this mode for devices without a timestamp unit (RT module).
v2-transparent-clock	Transparent Clock (one-step) function based on IEEE 1588-2008 (PTPv2) for devices with MM23 and MM33 media modules.

Table 10: Selecting a PTP mode.

☐ If no reference clock is available, specify a device as the reference clock and set its system time as accurately as possible.

Application Example

PTP is used to synchronize the time in the network but not with the real time as the PC is used to synchronize the time with a SNTP clock source on the Internet. As an SNTP client, the PC device gets the time from the NTP server via SNTP. The Magnum 12KX assigns PTP clock stratum 2 (PTPv1) or clock class 6 (PTPv2) to the time received from an NTP server. Thus the PC becomes the reference clock for the PTP synchronization and is the “preferred master”. The “preferred master” forwards the exact time signal via its connections to the RT module (e.g. PTP enabled devices). The device with the RT module receives the exact time signal at a connection of its RT module and thus has the clock mode “v1-boundary-clock”. The devices without an RT module have the clock mode “v1-simple-mode”.

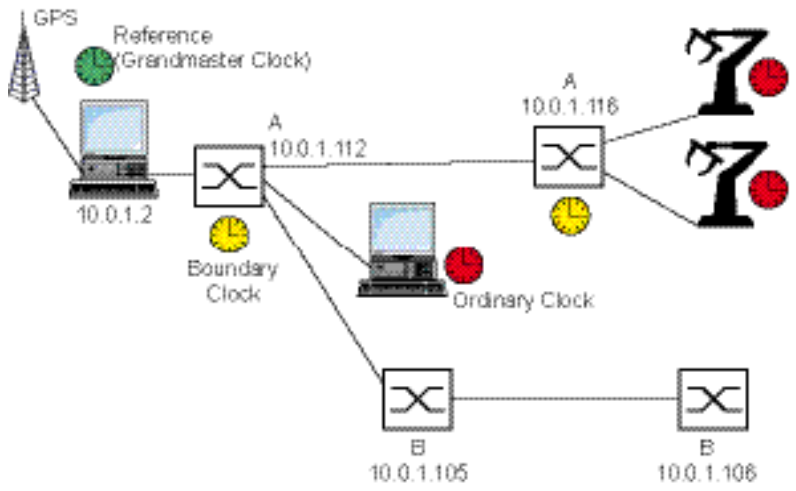


FIGURE 67 – Example of PTP synchronization. A = Device with RT module. B = Device without RT module.

Device	**10.0.1.112**	**10.0.1.116**	**10.0.1.105**	**10.0.1.106**
PTP Global				
Operation	on	on	on	on
Clock Mode	v1-boundary-clock	v1-boundary-clock	v1-simple-mode	v1-simple-mode
Preferred Master	true	false	false	false
SNTP				
Operation	on	off	off	off
Client Status	on	off	off	off
External server address	10.0.1.2	0.0.0.0	0.0.0.0	0.0.0.0
Server request interval	30	any	any	any
Accept SNTP Broadcasts	No	any	any	any
Server status	on	off	off	off

Anycast destination address	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
VLAN ID	1	1	1	1

Table 11: Settings for the example

The following configuration steps apply to the device with the IP address 10.0.1.112. Configure the other devices in the same way with the values from the table above.

☐ Enter the SNTP parameters.

Using the Web Interface:

☐ Select the `Time:SNTP` dialog.
☐ Activate SNTP globally in the “Operation” frame.
☐ Activate the SNTP client (client status) in the “Configuration SNTP Client” frame.
☐ In the “Configuration SNTP Client” frame, enter:
– “External server address”: 10.0.1.2
– “Request interval”: 30
– “Accept SNTP Broadcasts”: No

☐ Activate the SNTP server (server status) in the “Configuration SNTP Server” frame.
☐ In the “Configuration SNTP Server” frame, enter:
– “Anycast destination address”: 0.0.0.0
– “VLAN ID”: 1

☐ Click “Set” to temporarily save the entry in the configuration.

FIGURE 68 – Configuring the SNTP parameters.

Using the CLI Interface:

`enable`	**Switch to the Privileged EXEC mode.**
`configure`	**Switch to the Configuration mode.**
`sntp operation on`	**Switch on SNTP globally.**
`sntp operation client on`	**Switch on SNTP client.**
`sntp client server primary 10.0.1.2`	**Enter the IP address of the external SNTP server 10.0.1.2.**
`sntp client request-interval 30`	**Enter the value 30 seconds for the SNTP server request interval.**
`sntp client accept-broadcast off`	**Deactivate “Accept SNTP Broadcasts”.**
`sntp operation server on`	**Switch on SNTP server.**

`sntp anycast address 0.0.0.0`	**Enter the SNTP server Anycast destination address 0.0.0.0.**
`sntp anycast vlan 1`	**Enter the SNTP server VLAN ID 1.**

FIGURE 69 – Configuring the SNTP parameters using CLI.

☐ Enter the global PTP parameters.

Using the Web Interface:

☐ Select the `Time:PTP:Global` dialog.
☐ Activate the function in the “Operation IEEE 1588 / PTP” frame.
☐ Select `v1-boundary-clock` for “PTP version mode”.

☐ Click “Set” to temporarily save the entry in the configuration.

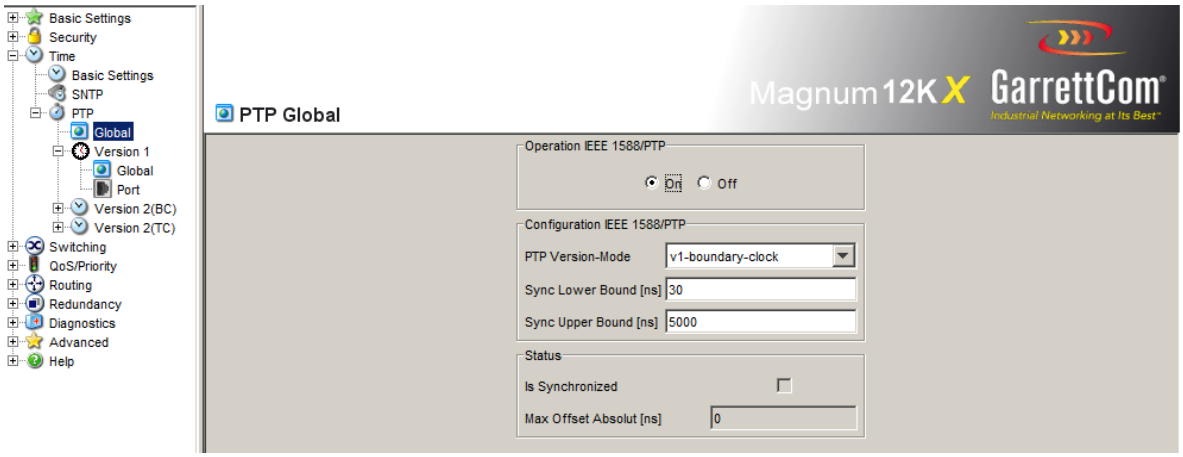


FIGURE 70 – Configuring the PTP parameters.

Using the CLI Interface:

`ptp operation enable`	**Switch on PTP globally.**
`ptp clock-mode v1-boundary-clock`	**Select PTP version and clock mode.**

FIGURE 71 – Configuring the PTP parameters using CLI.

☐ In this example, the device with the IP address 10.0.1.112 is the PTP reference clock. This device is the “Preferred Master”.

Using the Web Interface:

☐ Select the `Time:PTP:Version1:Global` dialog. NOTE – not all devices support PTP version 1 and PTP version 1 is not compatible with version 2. If the devices are not version 1 compatible, please use the Version 2 settings.

☐ In the “Operation IEEE 1588 / PTP” frame, select `true` for the “Preferred Master”.

☐ Click “Set” to temporarily save the entry in the configuration.

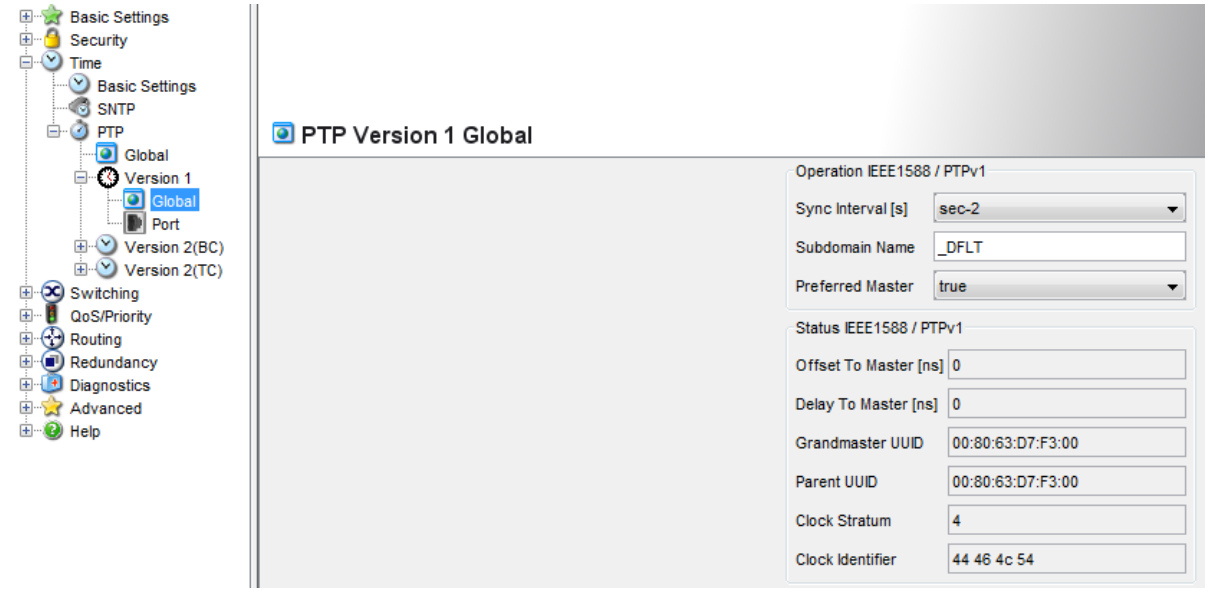


FIGURE 72 – Setting PTP

`ptp v1 preferred-master true` **Define this device as the “Preferred Master”.**

FIGURE 73 – Setting PTP master from CLI

☐ Get PTP to apply the parameters.

☐ In the `Time:PTP:Version1:Global` dialog, click on “Reinitialize” so that PTP applies the parameters entered.

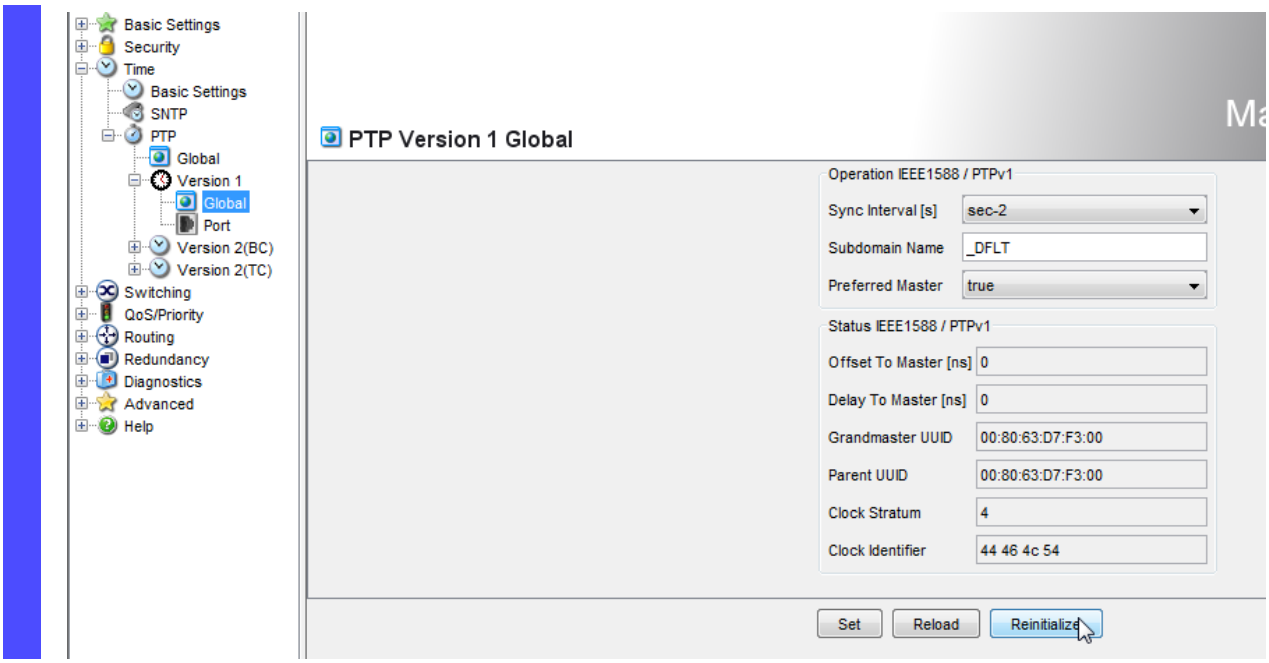


FIGURE 74 – Reinitializing PTP

`ptp v1 re-initialize` **Apply PTP parameters**.

FIGURE 75 – Reinitializing PTP from CLI

☐ Save the settings in the non-volatile memory.

☐ Select the `Basics: Load/Save` dialog.

☐ In the “Save” frame, select “To Device” for the location and click “Save” to permanently save the configuration in the active configuration.

`copy system:running-config nvram:startup-config` **Save the current configuration to the non-volatile memory**.

Interaction of PTP and SNTP

According to the PTP and SNTP standards, both protocols can exist in parallel in the same network. However, since both protocols affect the system time of the device, situations may occur in which the two protocols compete with each other.

Note: Configure the devices so that each device only receives the time from one source.
If the Magnum 12KX gets its time via PTP, enter the “External server address” 0.0.0.0 in the SNTP client configuration and do not accept SNTP Broadcasts.

If the Magnum 12KX gets its time via SNTP, make sure that the “best” clock is connected to the SNTP server. Then both protocols will get the time from the same server. The example below shows such an application.

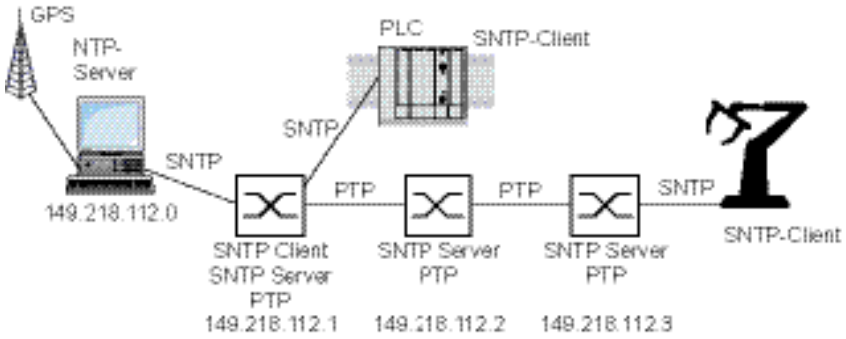


FIGURE 76 – Example of the coexistence of PTP and SNTP

Application Example

The requirements with regard to the accuracy of the time in the network are quite high, but the terminal devices only support SNTP.

Device	**149.218.112.1**	**149.218.112.2**	**149.218.112.3**
PTP			
Operation	on	on	on
Clock Mode	v1-boundary-clock	v1-boundary-clock	v1-boundary-clock
Preferred Master	false	false	false
SNTP			
Operation	on	on	on
Client Status	on	off	off
External server address	149.218.112.0	0.0.0.0	0.0.0.0
Server request interval	any	any	any
Accept SNTP Broadcasts	No	No	No

Server status	on	on	on
Anycast destination address	224.0.1.1	224.0.1.1	224.0.1.1
VLAN ID	1	1	1
Anycast send interval	30	30	30

Table 12: Settings for the example.

In the example, the PC (left device), as an SNTP client, gets the time from the NTP server via SNTP. The Magnum 12KX assigns PTP clock stratum 2 (PTPv1) or clock class 6 (PTPv2) to the time received from an NTP server. Thus the PC or the left device becomes the reference clock for the PTP synchronization. PTP is active for all three switches, thus enabling precise time synchronization between them. Since the other devices in the example only support SNTP, all three switches act as SNTP servers. If any PTP capable device was plugged in the network, the Magnum 12KX could participate with the switches in PTP and be synchronized.

Chapter 8

Network Load Control

To optimize the data transmission, the Magnum 12KX provides the following functions for controlling the network load:

- Settings for direct packet distribution (MAC address filter)
- Multicast settings
- Rate limiter
- Prioritization QoS
- Flow control
- Virtual LANs (VLANs)

Direct Packet Distribution

With direct packet distribution, a network administrator can help protect the Magnum 12KX as well as the network from unnecessary loads or bursts of traffic. The Magnum 12KX switch provides the following functions for direct packet distribution:

- Store-and-forward
- Multi-address capability
- Aging of learned addresses
- Static address entries
- Disabling the direct packet distribution

Store-and-forward

All data received by the Magnum 12KX is stored, and its validity is checked. Invalid and defective data packets (> 1,502 bytes or CRC errors) as well as fragments (< 64 bytes) are rejected. Valid data packets are forwarded by the Magnum 12KX.

Multi-Address Capability

The Magnum 12KX learns all the source addresses for a port. Only packets with

- unknown destination addresses
- these destination addresses or
- a multi/broadcast destination address

In the destination address field are sent to this port. The Magnum 12KX enters learned source addresses in its filter table.

The Magnum 12KX can learn up to 8,000 addresses. This is necessary if more than one terminal device is connected to one or more ports. It is thus possible to connect several independent subnetworks to the Magnum 12KX.

Aging of Learned Addresses

The Magnum 12KX monitors the age of the learned addresses. Address entries which exceed a particular age the aging time are deleted by the Magnum 12KX from its address table.
Data packets with an unknown destination address are flooded by the Magnum 12KX.
Data packets with known destination addresses are selectively transmitted by the Magnum 12KX.

Note: A reboot deletes the learned address entries.

☐ Select the `Switching:Global` dialog.

☐ Enter the aging time for all dynamic entries in the range from 10 to 630 seconds (unit: 1 second; default setting: 30).
In connection with the router redundancy, select a time ≥ 30 seconds.

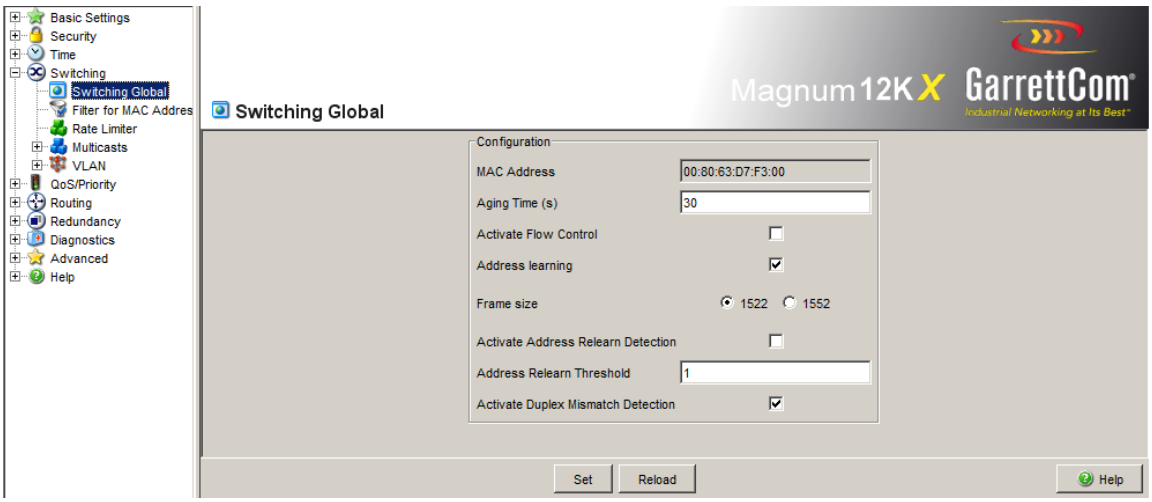


FIGURE 77 – Setting MAC address aging time and Switching Frame Size.

Entering Static Addresses

An important function of the Magnum 12KX is the filter function. It selects data packets according to defined patterns, known as filters. These patterns are assigned distribution rules. This means that a data packet received by a device at a port is compared with the patterns. If there is a pattern that matches the data packet, a device then sends or blocks this data packet according to the distribution rules at the relevant ports.

The following are valid filter criteria:

- Destination address
- Broadcast address
- Multicast address
- VLAN membership

The individual filters are stored in the filter table (Forwarding -Database, FDB). It consists of 3 parts: a static part and two dynamic parts.

- The management administrator describes the static part of the filter table (`dot1qStaticTable`).
- During operation, the Magnum 12KX is capable of learning which of its ports receive data packets from which source address. This information is written to a dynamic part (`dot1qTpFdbTable`).
- Addresses learned dynamically from neighboring agents and those learned via GMRP are written to the other dynamic part.

Addresses already located in the static filter table are automatically transferred to the dynamic part by the Magnum 12KX.
An address entered statically cannot be overwritten through learning.

Note: If the ring manager is active, it is not possible to make permanent unicast entries.

Note: This filter table allows the creation of up to 100 filter entries for Multicast addresses.

☐ Select the `Switching:Filters for MAC Addresses` dialog.

Each row of the filter table represents one filter. Filters specify the way in which data packets are sent. They are set automatically by the Switch (learned status) or created manually. Data packets whose destination address is entered in the table are sent from the receiving port to the ports marked in the table. Data packets whose destination address is not in the table are sent from the receiving port to all other ports. In the "Create filter" dialog set up new filters. The following status settings are possible:

- `learned`: The filter was created automatically by the Magnum 12KX.
- `invalid`: With this status delete a manually created filter.
- `permanent`: The filter is stored permanently in the Magnum 12KX or on the URL.
- `gmrp`: The filter was created by GMRP.
- `gmrp/permanent`: GMRP added further port markings to the filter after it was created by the administrator. The port markings added by the GMRP are deleted by a restart.
- `igmp`: The filter was created by IGMP Snooping.

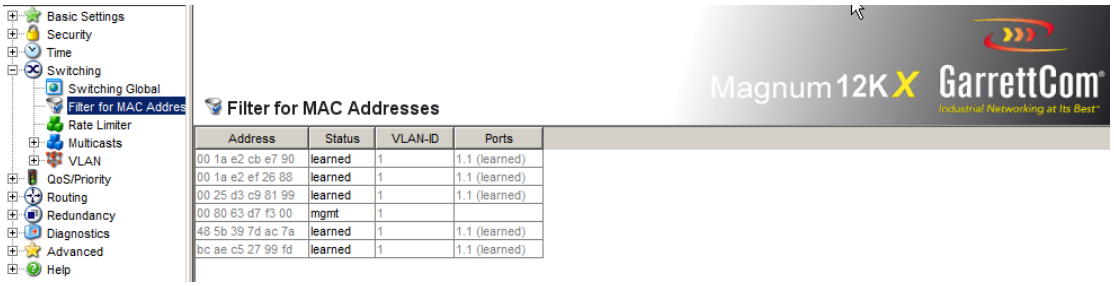


FIGURE 78 – Filters for MAC addresses.

To delete entries with the "learned" status from the filter table, select the `Basics:Restart` dialog and click "Reset MAC address table".

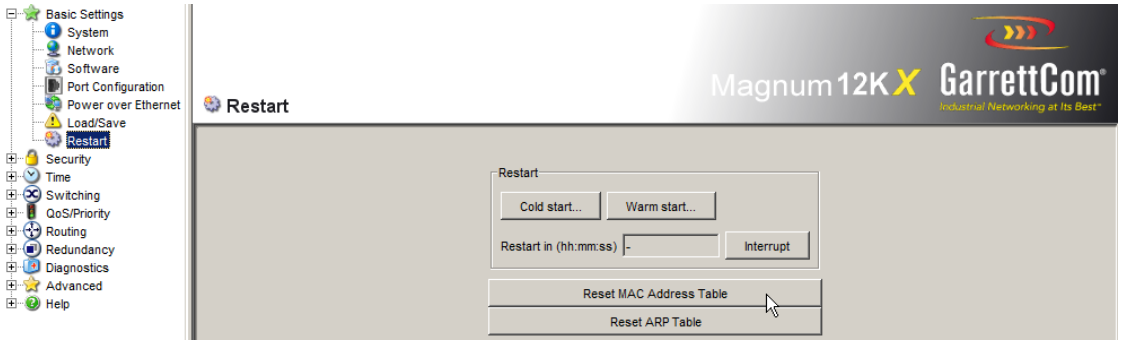


FIGURE 79 – Resetting MAC address Table.

Disabling the Direct Packet Distribution

To enable the observation of the data at all the ports, the Magnum 12KX allows the user to disable the learning of addresses. When the learning of addresses is disabled, the Magnum 12KX transfers all the data from all ports to all ports.

☐ Select the `Switching:Global` dialog.

UnCheck "Address Learning" to stop the address learning on all ports.

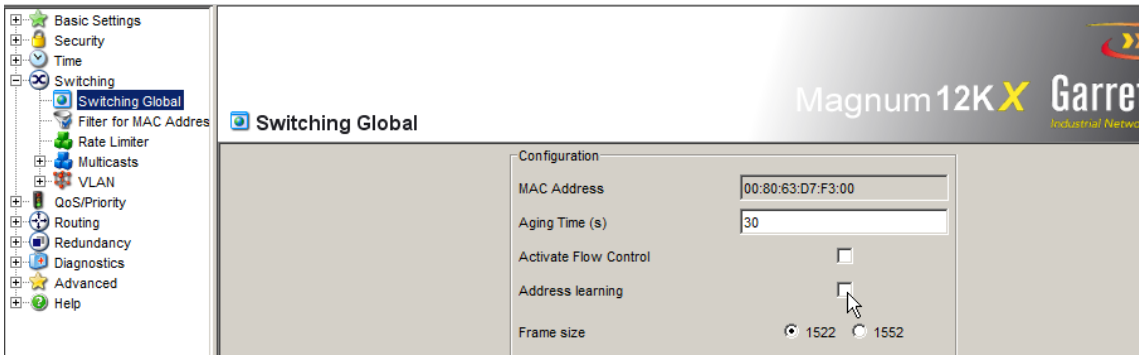


FIGURE 80 – To stop address leaning, uncheck the Address leaning box as shown above.

Multicast Applications

Description of the Multicast Application

The data distribution in the LAN differentiates between three distribution classes on the basis of the addressed recipients:

- Unicast - one recipient
- Multicast - a group of recipients
- Broadcast - every recipient that can be reached

In the case of a Multicast address, the Magnum 12KX forwards all data packets with a Multicast address to all ports. This leads to an increased bandwidth requirement.
Protocols such as GMRP and procedures such as IGMP Snooping enable the Magnum 12KX to exchange information via the direct transmission of Multicast data packets. The bandwidth requirement can be reduced by distributing the Multicast data packets only to those ports to which recipients of these Multicast packets are connected.

One can recognize IGMP Multicast addresses by the range in which the address lies:

- MAC Multicast Address
  01:00:5E:00:00:00 - 01:00:5E:FF:FF:FF
  (in mask form 01:00:5E:00:00:00/24)
- Class D IP Multicast address
  224.0.0.0 - 239.255.255.255
  (in mask form 224.0.0.0/4)

Example of a Multicast Application

The cameras for monitoring machines normally transmit their images to monitors located in the machine room and to the control room.

In an IP transmission, a camera sends its image data with a Multicast address via the network.

To prevent all the video data from slowing down the entire network, the Magnum 12KX uses the GMRP to distribute the Multicast address information. As a result, the image data with a Multicast address is only distributed to those ports that are connected to the associated monitors for surveillance.

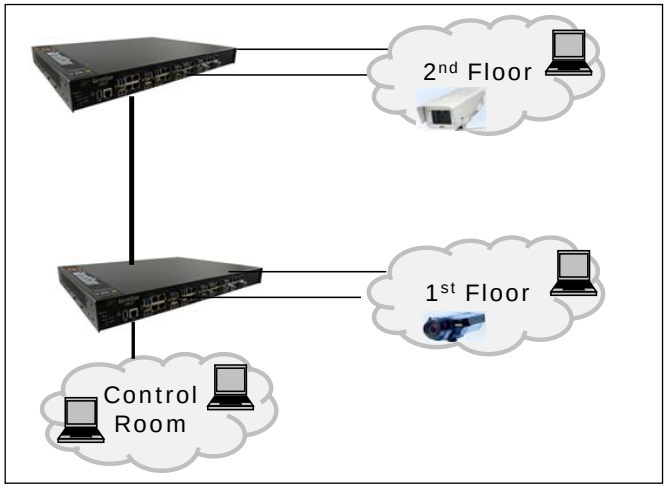


FIGURE 81 – Example: Video surveillance in machine rooms.

Description of IGMP Snooping

The Internet Group Management Protocol (IGMP) describes the distribution of Multicast information between routers and terminal devices on Layer 3.

Routers with an active IGMP function periodically send queries to find out which IP Multicast group members are connected to the LAN. Multicast group members reply with a Report message. This Report message contains all the parameters required by the IGMP. The router records the IP Multicast group address from the Report message in its routing table. The result of this is that it transfers frames with this IP Multicast group address in the destination field only in accordance with the routing table.

Devices which no longer want to be members of a Multicast group can cancel their membership by means of a Leave message (from IGMP version 2), and they do not transmit any more Report messages. In IGMP versions 1 and 2, the router removes the routing table entry if it does not receive any Report messages within a specified period of time (aging time).

If there are a number of routers with an active IGMP function in the network, then they work out among themselves (in IGMP version 2) which router carries out the Query function. If there is no router in the network, then a suitably equipped Switch can perform the Query function.

A Switch that connects a Multicast receiver with a router can evaluate the IGMP information with the aid of the IGMP Snooping procedure.

IGMP Snooping translates IP Multicast group addresses into MAC Multicast addresses, so that the IGMP functions can also be used by Layer 2 Switches. The Switch records the MAC addresses of the Multicast receivers, with are obtained via IGMP Snooping from the IP addresses, in the static address table. The Switch thus transmits these Multicast packets exclusively at the ports at which Multicast receivers are connected. The other ports are not affected by these packets.

A special feature of the Magnum 12KX is that the user can specify whether it should drop data packets with unregistered Multicast addresses, transmit them to all ports, or only to those ports at which the Magnum 12KX received query packets. Users have the option of additionally sending known Multicast packets to query ports.

Default setting: “Off”.

Setting IGMP Snooping

☐ Select the `Switching:Multicast:IGMP` dialog.

OPERATION (ENABLE / DISABLE)

The “Operation” frame allows the user to enable/disable IGMP Snooping globally for the entire device.
If IGMP Snooping is disabled, then

- the device does not evaluate Query and Report packets received, and
- it sends (floods) received data packets with a Multicast address as the destination address to all port

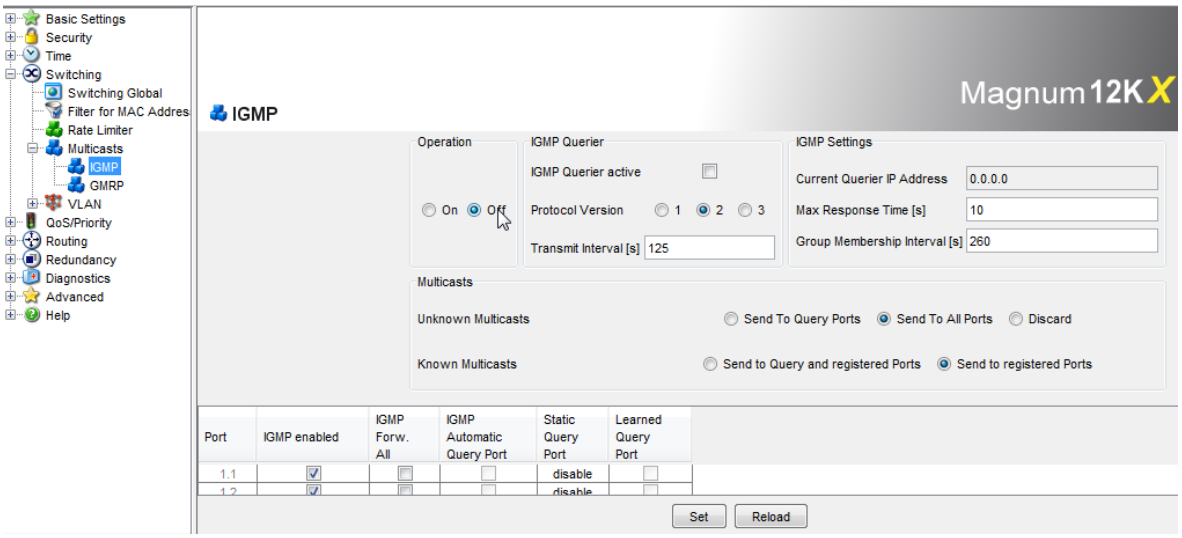


FIGURE 82 – Turning IGMP Operation On/Off

SETTINGS FOR IGMP QUERIER AND IGMP

With these frames global settings can be entered for the IGMP settings and the IGMP Querier function. Prerequisite: The IGMP Snooping function is activated globally.

IGMP Querier

"IGMP Querier active" allows enable/disable the Query function.

"Protocol version" allow selection of IGMP version 1, 2 or 3.

In "Send interval [s]" specify the interval at which the Magnum 12KX sends query packets (valid entries: 2-3,599 s, default setting: 125 s).

Note the connection between the parameters Max. Response -Time, Send Interval and Group Membership Interval.

IGMP-capable terminal devices respond to a query with a report message, thus generating a network load.
Select large sending intervals if the load on the network needs to be reduced and can accept the resulting longer switching times.
Select small sending intervals if short switching times is required and can accept the resulting network load.

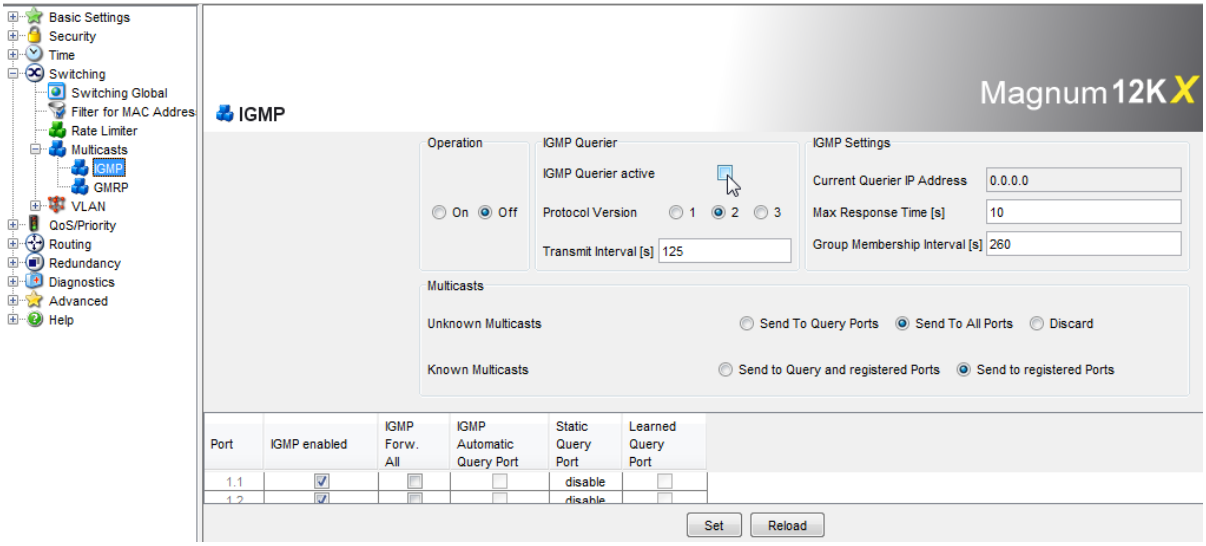


FIGURE 83 – IGMP Querier settings

IGMP Settings

"Current querier IP address" shows the IP address of the Magnum 12KX that has the query function.

In "Max. Response Time" specify the period within which the Multicast group members respond to a query (valid values: 1-3,598 s, default setting: 10 s).

Note the connection between the parameters Max. Response -Time, Send Interval and Group Membership Interval.

The Multicast group members select a random value within the maximum response time for their response, to prevent all the Multicast group members responding to the query at the same time.
Select a large value if the load on the network needs to be reduced and can accept the resulting longer switching times.
Select a small value if short switching times are required and can accept the resulting network load.

In "Group Membership Interval" specify the period for which a dynamic Multicast group remains entered in the Magnum 12KX if it does not receive any report messages (valid values: 3-3,600 s, default setting: 260 s).

Note the connection between the parameters Max. Response -Time, Send Interval and Group Membership Interval.

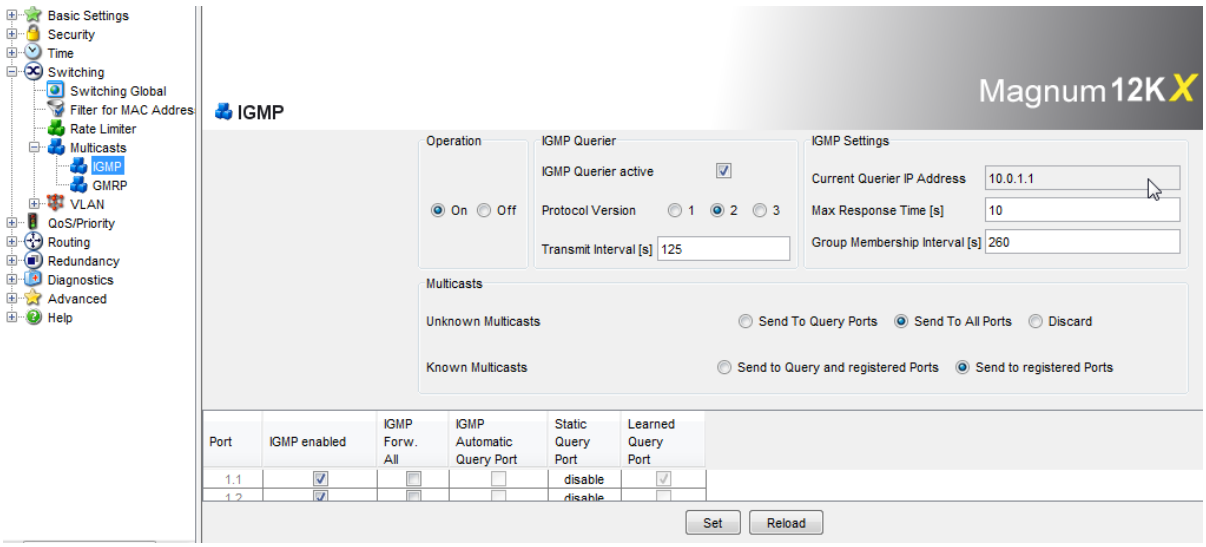


FIGURE 84 – IGMP Settings

Parameter Values

The parameters
- Max. Response Time,
- Send Interval and
- Group Membership Interval

have a relationship to each other:

Max. Response Time < Send Interval < Group Membership Interval.

If the entered values that contradict this relationship, the Magnum 12KX then replaces these values with a default value or with the last valid values.

Parameter	Protocol Version	Value range	Default setting
Max. Response Time,	1, 2, 3	1-25 seconds 1-3,598 seconds	10 seconds
Send Interval	1, 2, 3	2-3,599 seconds	125 seconds
Group Membership Interval	1, 2, 3	3-3,600 seconds	260 seconds

Table 13: Value range for Max. Response Time, Send Interval, Group Membership Interval.

MULTICASTS

With these frames the user can enter global settings for the Multicast functions.

Prerequisite: The IGMP Snooping function is activated globally.

Unknown Multicasts
In this frame determine how the Magnum 12KX in IGMP mode sends packets with known and unknown MAC/IP Multicast addresses that were not learned through IGMP Snooping.

“Unknown Muilticasts” allows users to specify how the Magnum 12KX transmits unknown Multicast packets:

- “Send to Query Ports”.
  The Magnum 12KX sends the packets with an unknown MAC/IP Multicast address to all query ports.
- “Send to All Ports”.
  The Magnum 12KX sends the packets with an unknown MAC/IP Multicast address to all ports.
- “Discard”.
  The Magnum 12KX discards all packets with an unknown MAC/IP Multicast address.

Note: The way in which unlearned Multicast addresses are handled also applies to the reserved IP addresses from the “Local Network Control Block” (224.0.0.0 - 224.0.0.255). This can have an effect on higher-level routing protocols.

Known Multicasts
In this frame determine how the Magnum 12KX in IGMP mode sends packets with known MAC/IP Multicast addresses that were learned through IGMP Snooping.

- “Send to query and registered ports”.
  The Magnum 12KX sends the packets with a known MAC/IP Multicast address to all query ports and to registered ports.
  This standard setting sends all Multicasts to all query ports and to registered ports. The advantage of this is that it works in most applications without any additional configuration.
  Application: “Flood and Prune” routing in PIM-DM.
- “Send to registered ports”.
  The Magnum 12KX sends the packets with a known MAC/IP Multicast address to registered ports.
  The advantage of this setting, which deviates from the standard, is that it uses the available bandwidth optimally through direct distribution. It requires additional port settings.
  Application: Routing protocol PIM-SM.

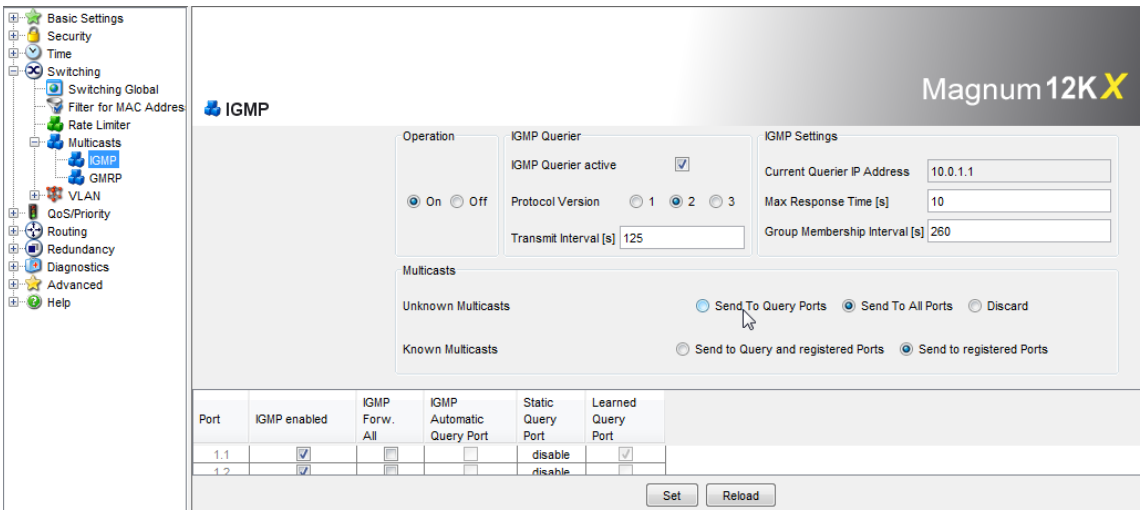


FIGURE 85 – Multicasts - setting Known and Unknown multicast settings.

SETTINGS PER PORT (TABLE)

- "IGMP on"
  This table column enables users to enable/disable the IGMP for each port when the global IGMP Snooping is enabled. Disabling the IGMP at a port prevents registration for this port.

- "IGMP Forward All"
  This table column enables usres to enable/disable the "Forward All" IGMP Snooping function when the global IGMP Snooping is enabled. With the "Forward All" setting, the Magnum 12KX sends to this port all data packets with a Multicast address in the destination address field.

  Note: If a number of routers are connected to a subnetwork, IGMP version 1 must be used so that all the routers receive all the IGMP reports.

  Note: If IGMP version 1 is used in a subnetwork, IGMP version 1 must be used in the entire network.

- "IGMP Automatic Query Port"
  This table column shows which ports the Magnum 12KX has learned as query ports, if "automatic" is selected in "Static Query Port".

- "Static Query Port"
  The Magnum 12KX sends IGMP report messages to the ports at which it receives IGMP queries (disable=default setting).
  This column allows sending IGMP report messages to:
  other selected ports (enable) or connected
  devices (automatic).

- "Learned Query Port"
  This table column shows at which ports the Magnum 12KX has received IGMP queries, if "disable" is selected in "Static Query Port".

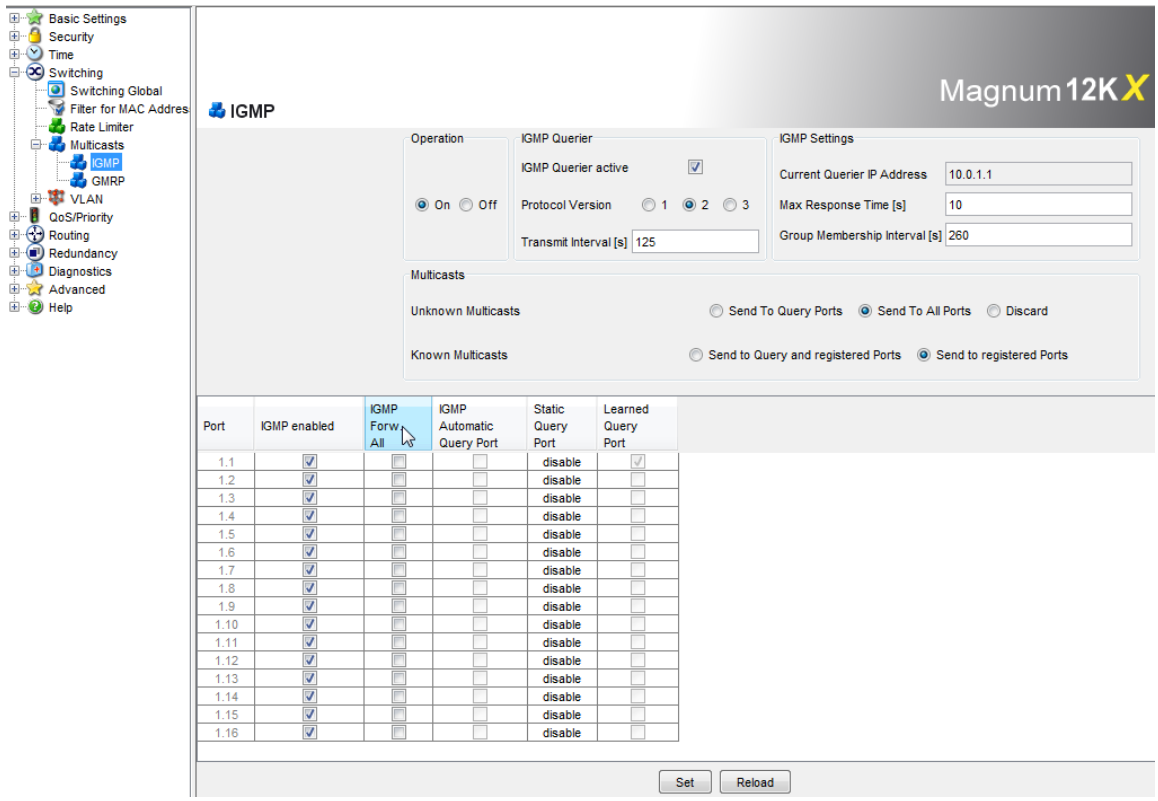


FIGURE 86 – IGMP Per Port configuration.

GARP Multicast Registration Protocol (GMRP)

The GARP Multicast Registration Protocol (GMRP) describes the distribution of data packets with a Multicast address as the destination address on Layer 2.

Devices that want to receive data packets with a Multicast address as the destination address use the GMRP to perform the registration of the Multicast address. For a Switch, registration involves entering the Multicast address in the filter table. When a Multicast address is entered in the filter table, the Switch sends this information in a GMRP packet to all the ports. Thus the connected Switches know that they have to forward this Multicast address to this Switch. The GMRP enables packets with a Multicast address in the destination address field to be sent to the ports entered. The other ports are not affected by these packets.

Data packets with unregistered Multicast addresses are sent to all ports by the Switch.

Default setting: “Off”.

Setting GMRP

☐ Select the `Switching:Multicasts:GMRP` dialog.

OPERATION

The “Operation” frame enables GMRP globally for the entire device.

It GMRP is disabled, then

- the Magnum 12KX does not generate any GMRP packets,
- does not evaluate any GMRP packets received, and
- sends (floods) received data packets to all ports.

The Magnum 12KX is transparent for received GMRP packets, regardless of the GMRP setting.

SETTINGS PER PORT (TABLE)

- “GMRP”
  This table column shows how to enable/disable the GMRP for each port when the GMRP is enabled globally. When the GMRP at a port is switched off, no registrations can be made for this port, and GMRP packets cannot be forwarded at this port.

- “GMRP Service Requirement”
  Devices that do not support GMRP can be integrated into the Multicast addressing by means of
  - a static filter address entry on the connecting port.
  - selecting “Forward all groups” in the table column “GMRP Service Requirement”. The Magnum 12KX enters ports with the selection “Forward all groups” in all Multicast filter entries learned via GMRP.

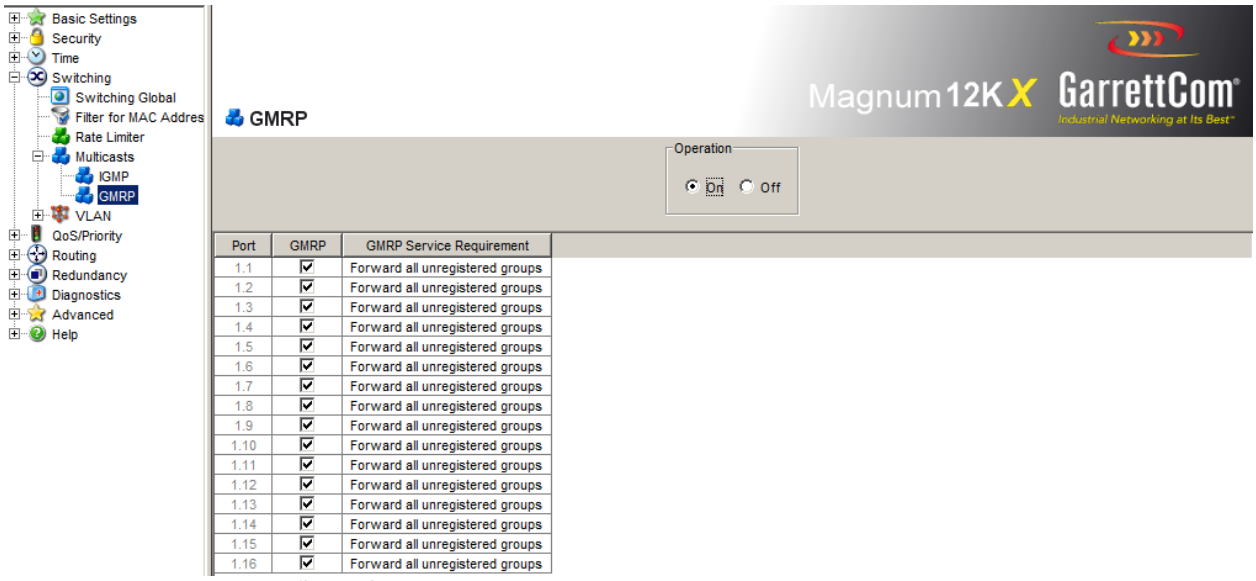


FIGURE 87 – GMRP configuration.

Description of the Rate Limiter

The Magnum 12KX can limit the rate of message traffic during periods of heavy traffic flow.

Entering a limit rate for each port specifies the amount of traffic the Magnum 12KX is permitted to transmit and receive.

If the data load transmitted at this port exceeds the maximum load entered, the Magnum 12KX will discard the excess data at this port.

A global setting enables/disables the rate limiter function at all ports.

Note: The limiter functions work exclusively on layer 2 and serve the purpose of limiting the effects of storms of those frame types (typically broadcasts) that the Switch floods. The limiter function ignores any protocol information of higher layers like IP or TCP. This may affect e.g., TCP traffic.

These effects can be minimized by:

- applying the limiter function only to particular frame types (e.g., to broadcasts, multicasts and unicasts with an unlearned destination address) and excluding unicasts with a learned destination address from the limitation,
- using the egress limiter function instead of the ingress limiter function because the former cooperates slightly better with TCP's flow control (reason: frames buffered by the internal switching buffer),
- increasing the aging time for learned unicast destination addresses.

Rate Limiter Settings

☐ Select the `Switching:Rate Limiter` dialog.

- "Ingress Limiter (kbit/s)" allows enable or disable the ingress limiter function for all ports and to select the ingress limitation on all ports (either broadcast packets only or broadcast packets and Multicast packets).
- "Egress Limiter (Pkt/s)" allows enable or disable the egress limiter function for broadcasts on all ports.

Setting options per port:

- Ingress Limiter Rate for the packet types selected in the Ingress Limiter frame:
  - = 0, no ingress limit at this port.
  - > 0, maximum incoming traffic rate in kbit/s that is allowed to be sent at this port.
- Egress Limiter for broadcast packets:
  - = 0, no rate limit for outbound broadcast packets at this port.
  - > 0, maximum number of outgoing broadcasts per second sent at this port.

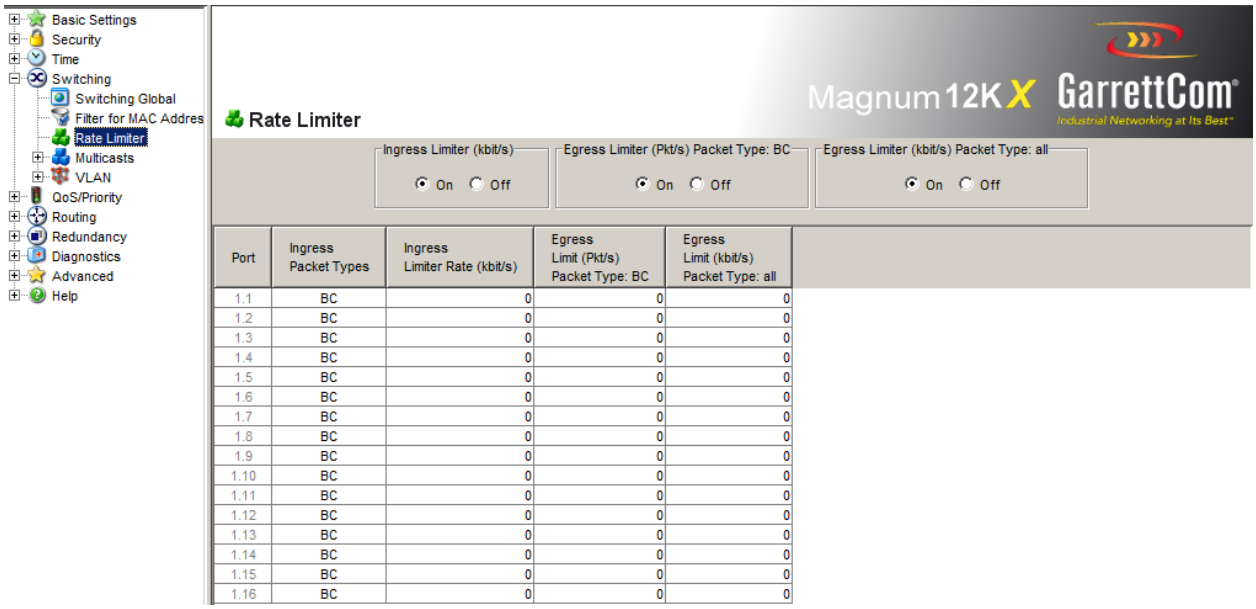


FIGURE 88 – Rate Limiting.

Chapter 9

Quality of Service (QoS)

QoS and Prioritization

QoS is specified in the IEEE 802.1p and IEEE 802.1q standards. QoS is important in network environments where there are time-critical applications, such as voice transmission or video conferencing, which can be adversely effected by packet transfer delays or other latency in a network. Most switches today implement buffers to queue incoming packets as well as outgoing packets. In a queue mechanism, normally the packet which comes in first leaves first (FIFO) and all the packets are serviced accordingly. Imagine, if each packet had a priority assigned to it. If a packet with a higher priority than other packets were to arrive in a queue, the packet would be given a precedence and moved to the head of the queue and would go out as soon as possible. The packet is thus preempted from the queue and this method is called preemptive queuing.

Preemptive queuing makes sense if there are several levels of priorities, normally more than two. If there are too many levels, then the system has to spend a lot of time managing the preemptive nature of queuing. IEEE 802.1p defines and uses eight levels of priorities. The eight levels of priority are enumerated 0 to 7, with 0 the lowest priority and 7 the highest.

To make the preemptive queuing possible, most switches implement at least two queue buffers. The Magnum 6K family of switches has two priority queues, 1 (low) and 0 (high).When tagged packets enter a switch port, the switch responds by placing the packet into one of the two queues, and depending on the precedence levels the queue could be rearranged to meet the QoS requirements.

> QoS refers to the level of preferential treatment a packet receives when it is being sent through a network. QoS allows time sensitive packets such as voice and video, to be given priority over time insensitive packets such as data. Differentiated Services (DiffServ or DS) are a set of technologies defined by the IETF (Internet Engineering Task Force) to provide quality of service for traffic on IP networks.

This function prevents time-critical data traffic such as language/video or real-time data from being disrupted by less time-critical data traffic during periods of heavy traffic. By assigning high traffic classes for time-critical data and low traffic classes for less time-critical data, this provides optimal data flow for time-critical data traffic.

The Magnum 12KX supports eight priority queues (traffic classes in compliance with IEEE 802.1D). The assignment of received data packets to these classes is performed by

- Access Control Lists, MAC- or IP-based ACLs
- the priority of the data packet contained in the VLAN tag when the receiving port was configured to “trust dot1p”.
- the QoS information (ToS/DiffServ) contained in the IP header when the receiving port was configured to “trust ip-dscp”.

- the port priority when the port was configured to “no trust”.
- the port priority when receiving non-IP packets when the port was configured to “trust ip-dscp”.
- the port priority when receiving data packets without a VLAN tag and when the port was configured to “trust dot1p”.

  Default setting: “trust dot1p”.

The Magnum 12KX considers the classification mechanisms in the sequence shown above. This means that access control lists always have priority over the following mechanisms. Access control lists can prioritize the data packets with reference to Layer 2, Layer 3 and Layer 4 (e.g. MAC addresses, IP addresses, protocols, TCP/UDP ports).

Data packets can contain prioritizing/QoS information:

- VLAN priority based on IEEE 802.1Q/ 802.1D (Layer 2)
- Type of Service (ToS) or DiffServ (DSCP) for IP packets (Layer 3)

VLAN tagging

The VLAN tag is integrated into the MAC data frame for the VLAN and Prioritization functions in accordance with the IEEE 802 1Q standard. The VLAN tag consists of 4 bytes. It is inserted between the source address field and the type field.

For data packets with a VLAN tag, the Magnum 12KX evaluates
- the priority information and
- the VLAN information if VLANs have been setup.

Data packets with VLAN tags containing priority information but no VLAN information (VLAN ID = 0), are known as Priority Tagged Frames.

Priority entered	Traffic class (default setting)	IEEE 802.1D traffic type
0	2	Best effort (default)
1	0	Background
2	1	Standard
3	3	Excellent effort (business critical)
4	4	Controlled load (streaming multimedia)
5	5	Video, less than 100 milliseconds of latency and jitter
6	6	Voice, less than 10 milliseconds of latency and jitter
7	7	Network control reserved traffic

Table 14: Assignment of the priority entered in the tag to the traffic classes

Note: Network protocols and redundancy mechanisms use the highest traffic class 7. Therefore, select other traffic classes for application data.

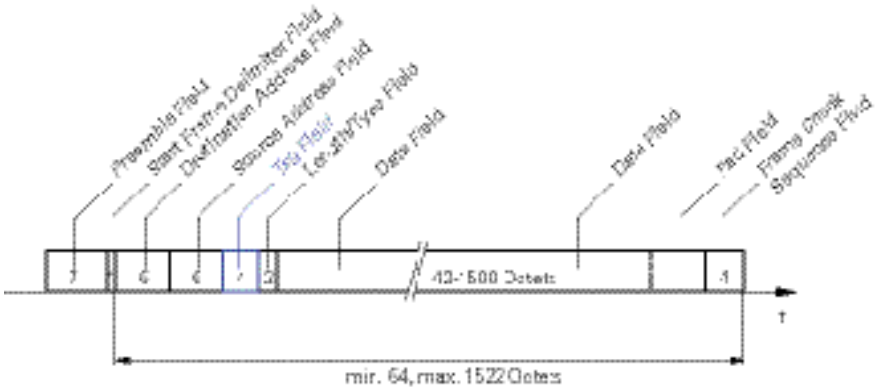


FIGURE 89 – Ethernet data packet with tag

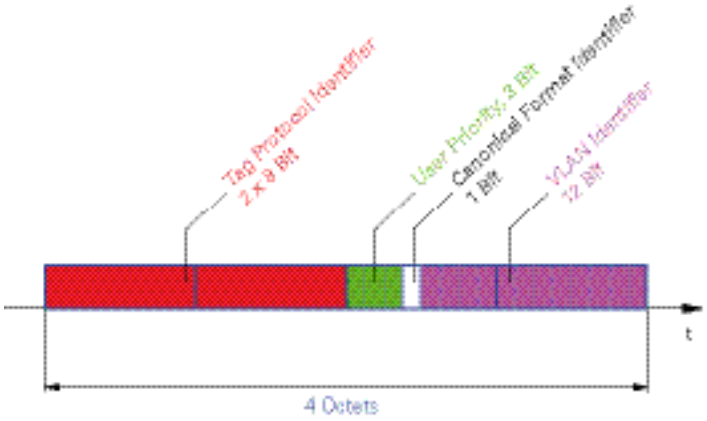


FIGURE 90 – Tag format

When using VLAN prioritizing, note the following special features:

- End-to-end prioritizing requires the VLAN tags to be transmitted to the entire network, which means that all network components must be VLAN-capable.
- Routers cannot receive or send packets with VLAN tags via port-based router interfaces.

IP ToS / DiffServ

TYPE of Service

The Type of Service (ToS) field in the IP header (see table **Error! Reference source not found.**) has been part of the IP protocol from the start, and it is used to differentiate various services in IP networks. Even back then, there were ideas about differentiated treatment of IP packets, due to the limited bandwidth available and the unreliable connection paths. Because of the continuous increase in the available bandwidth, there was no need to use the ToS field. Only with the real-time requirements of today's networks has the ToS field become significant again. Selecting the ToS byte of the IP header enables the user to differentiate between different services. However, this field is not widely used in practice.

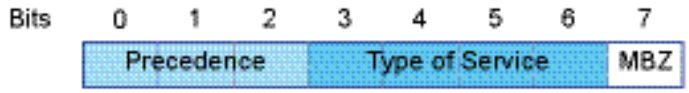


FIGURE 91 – ToS field in packet header

Bits (0-2): IP Precedence Defined	Bits (3-6): Type of Service Defined	Bit (7)
111 - Network Control	0000 - [all normal]	0 - Must be zero
110 - Internetwork Control	1000 - [minimize delay]	
101 - CRITIC / ECP	0100 - [maximize throughput]	
100 - Flash Override	0010 - [maximize reliability]	
011 - Flash	0001 - [minimize monetary cost]	
010 - Immediate		
001 - Priority		
000 - Routine		

Table 15: ToS field in the IP header

Differentiated Services

The newly defined Differentiated Services field in the IP header often known as the DiffServ code point or DSCP, replaces the ToS field and is used to mark the individual packets with a DSCP. Here the packets are divided into different quality classes. The first 3 bits of the DSCP are used to divide the packets into classes. The next 3 bits are used to further divide the classes on the basis of different criteria. In contrast to the ToS byte, DiffServ uses six bits for the division into classes. This results in up to 64 different service classes.

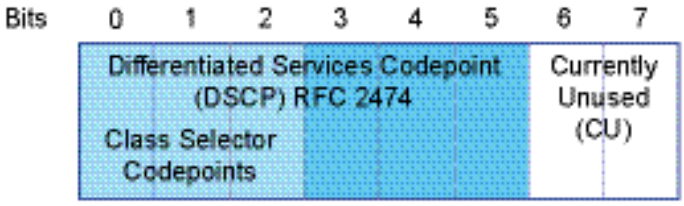


FIGURE 92 – Differentiated Services field in the IP header

The different DSCP values get the Magnum 12KX to employ a different forwarding behavior, namely Per-Hop Behavior (PHB). PHB classes:

- Class Selector (CS0-CS7): For reasons of compatibility to TOS/IP Precedence
- Expedited Forwarding (EF): Premium service.
  Reduced delay, jitter + packet loss (RFC-2598)
- Assured Forwarding (AF): Provides a differentiated schema for handling different data traffic (RFC-2597).
- Default Forwarding/Best Effort: No particular prioritizing.

The PHB class selector assigns the 7 possible IP precedence values from the old ToS field to specific DSCP values, thus ensuring the downwards compatibility.

ToS Meaning	Precedence Value	Assigned DSCP
Network Control	111	CS7 (111000)
Internetwork Control	110	CS6 (110000)
Critical	101	CS5 (101000)
Flash Override	100	CS4 (100000)
Flash	011	CS3 (011000)
Immediate	010	CS2 (010000)
Priority	001	CS1 (001000)
Routine	000	CS0 (000000)

Table 16: Assigning the IP precedence values to the DSCP value

DSCP value	DSCP name	Traffic class (default setting)
0	Best Effort /CS0	2
1-7		2
8	CS1	0
9,11,13,15		0
10,12,14	AF11,AF12,AF13	0
16	CS2	1
17,19,21,23		1
18,20,22	AF21,AF22,AF23	1
24	CS3	3
25,27,29,31		3
26,28,30	AF31,AF32,AF33	3
32	CS4	4
33,35,37,39		4
34,36,38	AF41,AF42,AF43	4
40	CS5	5
41,42,43,44,45,47		5
46	EF	5
48	CS6	6
49-55		6
56	CS7	7
57-63		7

Table 17: Mapping the DSCP values onto the traffic classes

Management prioritization

To have full access to the management of the Magnum 12KX, even in situations of high network load, the Magnum 12KX enables the user to prioritize management packets.
In prioritizing management packets (SNMP, Telnet, etc.), the Magnum 12KX sends the management packets with priority information.

- On Layer 2 the Magnum 12KX modifies the VLAN priority in the VLAN tag.
  For this function to be useful, the configuration of the corresponding ports must permit the sending of packets with a VLAN tag.

- On Layer 3 the Magnum 12KX modifies the IP-DSCP value.

Handling of Received Priority Information

The Magnum 12KX provides 3 options for each port for selecting how it handles received data packets that contain priority information.

- trust dot1p
  The Magnum 12KX assigns VLAN-tagged packets to the different traffic classes according to their VLAN priorities. The assignment is based on the pre-defined table. This assignment can be modified. The Magnum 12KX assigns the port priority to packets that it receives without a tag.
- untrusted
  The Magnum 12KX ignores the priority information in the packet and always assigns the packets the port priority of the receiving port.
- trust ip-dscp
  The Magnum 12KX assigns the IP packets to the different traffic classes according to the DSCP value in the IP header, even if the packet was also VLAN-tagged. The assignment is based on the pre-defined values. This assignment can be modified.

The Magnum 12KX prioritizes non-IP packets according to the port priority.

Handling of Traffic Classes

For the handling of traffic classes, the Magnum 12KX provides:

- Strict Priority
- Weighted Fair Queuing
- Strict Priority combined with Weighted Fair Queuing

Default setting: Strict Priority.

- Description of Strict Priority
  With the Strict Priority setting, the Magnum 12KX first transmits all data packets that have a higher traffic class before transmitting a data packet with the next highest traffic class. The Magnum 12KX transmits a data packet with the lowest traffic class only when there are no other data packets remaining in the queue. In some cases, a high level of data traffic can prevent packets with lower traffic classes from being sent.
  In applications that are time- or latency-critical, such as VoIP or video, this method ensures that high-priority data is sent immediately.

Description of Weighted Fair Queuing

With Weighted Fair Queuing, also known as Weighted Round Robin (WRR), the user can assign a minimum or reserved bandwidth to each traffic class. The result of this is that when the network is very busy, even data packets with a low priority are transmitted.

The weighting values range from 0% to 100% of the available bandwidth, in steps of 5%.

- A weighting of 0 is equivalent to a "no bandwidth" setting.
- The sum of the individual bandwidths may add up to 100%.

If Weighted Fair Queuing is assigned to all traffic classes, the entire bandwidth for the corresponding port is available.

When Weighted Fair Queuing is combined with Strict Priority, make sure that the highest traffic class of Weighted Fair Queuing is smaller than the lowest traffic class of Strict Priority.
In this case, a high Strict Priority network load can significantly reduce the bandwidth available for Weighted Fair Queuing.

Maximum Bandwidth

By entering a maximum bandwidth limit the bandwidth for each traffic class to a maximum value, regardless of whether "Weighted Fair Queuing" or "Strict Priority" was selected.

- Weighted Fair Queuing requires that the maximum bandwidth is at least as big as the minimum bandwidth.
- With "Strict Priority", individual high-priority packets with low latency are processed. If the maximum bandwidth is configured to a value less than 100%, even data packets will lower traffic classes can be sent in periods of high-priority overloading.

  The weighting values range from 0% to 100% of the available bandwidth, in steps of 5%.

Description of Traffic Shaping

With Traffic Shaping there is the option of restricting the maximum bandwidth of an interface.

The values for the bandwidth restriction range from 0% to 95%, in steps of 5%.

- The value "0" is equivalent to a "no bandwidth restriction" setting.
- The value "95" means that 95% of the bandwidth is available.

If the bandwidth set is temporarily exceeded, the Magnum 12KX saves the data and sends it when the bandwidth load has decreased again. Traffic Shaping thus smooth out any overload situations.

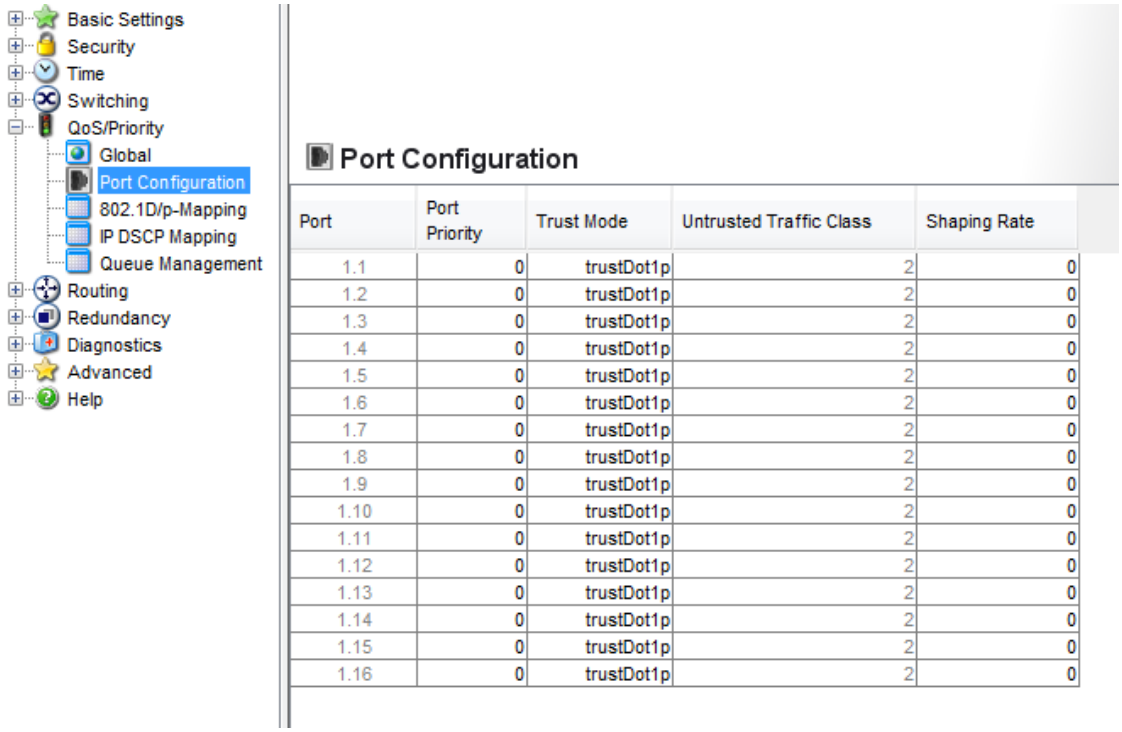
If Traffic Shaping is active on an interface, the Magnum 12KX ignores the bandwidths reserved for Weighted Fair Queuing.

Setting prioritization

Assigning the Port Priority

☐ Select the `QoS/Priority:Port Configuration` dialog.
☐ In the “Port Priority” column, it is possible to specify the priority (0-7) with which the Magnum 12KX sends data packets which it receives without a VLAN tag at this port.

Note: If VLANs have been set up, pay attention to the “Transparent mode” (see `Switching:VLAN:Global`)



Port	Port Priority	Trust Mode	Untrusted Traffic Class	Shaping Rate
1.1	0	trustDot1p	2	0
1.2	0	trustDot1p	2	0
1.3	0	trustDot1p	2	0
1.4	0	trustDot1p	2	0
1.5	0	trustDot1p	2	0
1.6	0	trustDot1p	2	0
1.7	0	trustDot1p	2	0
1.8	0	trustDot1p	2	0
1.9	0	trustDot1p	2	0
1.10	0	trustDot1p	2	0
1.11	0	trustDot1p	2	0
1.12	0	trustDot1p	2	0
1.13	0	trustDot1p	2	0
1.14	0	trustDot1p	2	0
1.15	0	trustDot1p	2	0
1.16	0	trustDot1p	2	0

FIGURE 93 – QoS Port Configuration

`enable`	**Switch to the Privileged EXEC mode.**
`Configure`	**Switch to the Configuration mode.**
`Interface 1/1`	**Switch to the Interface Configuration mode of interface 1/1.**
`vlan priority 3`	**Assign port priority 3 to interface 1/1.**
`exit`	**Switch to the Configuration mode.**

FIGURE 94 – QoS Port Configuration using CLI

Assigning the VLAN Priority to the Traffic Classes

☐ Select the `QOS/Priority:802.1D/p-Mapping` dialog.
☐ In the "Traffic Class" column, enter the desired values.

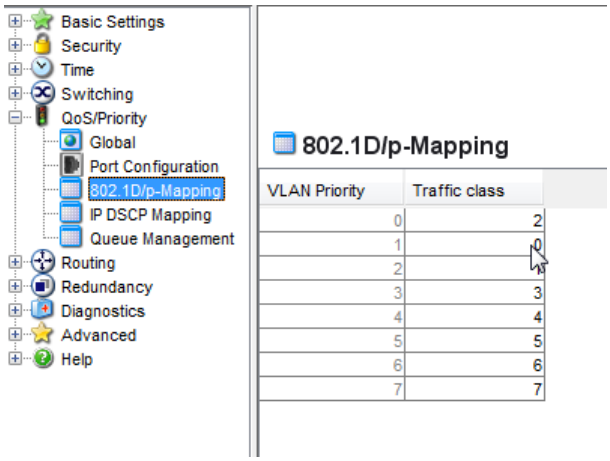


FIGURE 95 – QoS priority mapping

`enable`	**Switch to the Privileged EXEC mode.**
`configure`	**Switch to the Configuration mode.**
`classofservice dot1p-mapping 0 2`	**Assign traffic class 2 to VLAN priority 0.**
`classofservice dot1p-mapping 1 2`	**Also assign traffic class 2 to VLAN priority 1.**
`exit`	**Switch to the privileged EXEC mode.**
`show classofservice dot1p-mapping`	**Display the assignment.**

```
 User Priority    Traffic Class
 -------------    -------------
       0                2
       1                2
       2                0
       3                1
       4                2
       5                2
       6                3
       7                3
```

FIGURE 96 – QoS priority mapping using CLI

- Always assign the port priority to received data packets

`enable`	**Switch to the Privileged EXEC mode.**
`configure`	**Switch to the Configuration mode.**
`interface 1/1`	**Switch to the Interface Configuration mode of interface 1/1.**
`no classofservice trustvlan priority 1`	**Assign the "no trust" mode to the interface. Set the port priority to 1.**
`exit`	**Switch to the Configuration mode.**
`exit`	**Switch to the privileged EXEC mode.**

`show classofservice trust 1/1`	**Display the trust mode on interface 1/1.**

```
Class of Service Trust Mode: Untrusted

Untrusted Traffic Class: 4
```

FIGURE 97 – QoS port priority to received data packets

Assigning the traffic class to a DSCP

☐ Select the `QOS/Priority:IP DSCP Mapping` dialog.
☐ In the "Traffic Class" column, enter the desired values.

`enable`	**Switch to the Privileged EXEC mode.**
`configure`	**Switch to the Configuration mode.**
`classofservice ip-dscp-mapping cs1 1`	**Assign traffic class 1 to DSCP CS1.**
`show classofservice ip-dscp-mapping`	

```
    IP DSCP       Traffic Class
-------------     -------------
  0(be/cs0)           2
  1                   2
  .
  .
  8(cs1)              1
  .
```

FIGURE 98 – QoS mapping traffic class to DSCP using CLI

Always assign the DSCP priority to received IP data packets per interface

`enable`	**Switch to the Privileged EXEC mode.**
`configure`	**Switch to the Configuration mode.**
`interface 6/1` `classofservice trust ip-dscp`	**Switch to the interface configuration mode of interface 6/1. Assign the "trust ip-dscp" mode to the interface.**
`exit`	**Switch to the Configuration mode.**
`exit`	**Switch to the privileged EXEC mode.**
`show classofservice trust 6/1`	**Display the trust mode on interface 6/1.**

```
Class of Service Trust Mode: IP DSCP

Non-IP Traffic Class: 2
```

FIGURE 99 – QoS DSCP priority to received IP data packet mapping using CLI

Always assign the DSCP priority to received IP data packets globally

☐ Select the `QoS/Priority:Global` dialog.
☐ Select `trustIPDSCP` in the "Trust Mode" line.

`enable`	**Switch to the Privileged EXEC mode.**
`configure`	**Switch to the Configuration mode.**
`classofservice trust ip-dscp`	**Assign the "trust ip-dscp" mode globally.**
`exit`	**Switch to the Configuration mode.**
`exit`	**Switch to the privileged EXEC mode.**
`show classofservice trust`	**Display the trust mode.**

```
Class of Service Trust Mode: IP DSCP
```

FIGURE 100 – QoS DSCP priority to received IP data packet mapping globally using CLI

Configuration of Weighted Fair Queuing and Traffic Shaping

`enable`	**Switch to the Privileged EXEC mode.**
`configure`	**Switch to the Configuration mode.**
`no cos-queue strict 0 1 2 3 4 5`	**Switches off Strict Priority for traffic classes 0 to 5 and thus switches on Weighted Fair Queuing. Traffic classes 6 and 7 remain in Strict Priority mode.**
`cos-queue min-bandwidth 10 10 15 15 20 30 0 0`	**Assigns the weighting to the Weighted Fair Queuing traffic classes. In the case of Strict Priority, because the Magnum 12KX first transmits all the data packets with a high priority, the weighting 0 can be entered for the Strict Priority traffic classes and distribute 100% among the remaining traffic classes. The Magnum 12KX distributes the remaining bandwidth in accordance with the percentage weighting.**
`cos-queue max-bandwidth 20 20 20 20 20 30 30 30`	**Assign a maximum bandwidth to all traffic classes (Shaping). Because the two Strict Priority traffic classes are limited to a maximum of 30%, the remaining queues have at least 40% of the bandwidth at their disposal. The Magnum 12KX immediately sends Strict Priority data up to a maximum bandwidth of 30%.**
`exit`	**Switch to the privileged EXEC mode.**
`show interfaces cos-queue`	**Display the configuration.**

```
Global Configuration
Interface Shaping Rate..................... 0

Queue Id   Min. Bandwidth   Max. Bandwidth   Scheduler Type
--------   --------------   --------------   --------------
0          10               20               Weighted
1          10               20               Weighted
2          15               20               Weighted
3          15               20               Weighted
4          20               20               Weighted
```

```
5          30              30              Weighted
6          0               30              Strict
7          0               30              Strict
```

FIGURE 101 – Weighted Fail Queuing and traffic shaping using CLI

Configuration of Traffic Shaping on an interface

`enable`	**Switch to the Privileged EXEC mode.**
`configure`	**Switch to the Configuration mode.**
`interface 1/2`	**Switch to the interface configuration mode for interface 1/2.**
`traffic-shape 50`	**Restricts the maximum bandwidth of interface 1/2 to 50%.**
`exit`	**Switch to the Configuration mode.**
`exit`	**Switch to the privileged EXEC mode.**
`show interfaces cos-queue 1/2`	**Display the configuration of interface 1/2.**

```
Interface..................................... 1/2
Interface Shaping Rate........................ 50

Queue Id   Min. Bandwidth   Max. Bandwidth   Scheduler Type
--------   --------------   --------------   --------------
0          10               20               Weighted
1          10               20               Weighted
2          15               20               Weighted
3          15               20               Weighted
4          20               20               Weighted
5          30               30               Weighted
6          0                30               Strict
7          0                30               Strict
```

FIGURE 102 – Weighted Fail Queuing and traffic shaping for an interface using CLI

Configuring Layer 2 management priority

Configure the VLAN ports to which the Magnum 12KX sends management packets as a member of the VLAN that sends data packets with a tag.

- ☐ Select the QoS/Priority:Global dialog.
- ☐ In the line VLAN priority for management packets enter the value of the VLAN priority.

`enable`	**Switch to the Privileged EXEC mode.**
`network priority dot1p-vlan 7`	**Assign the value 7 to the management priority so that management packets with the highest priority are sent.**
`exit`	**Switch to the privileged EXEC mode.**

`show network`	**Displays the management VLAN priority.**

```
System IP Address............................. 10.0.1.116
Subnet Mask................................... 255.255.255.0
Default Gateway............................... 10.0.1.200
Burned In MAC Address......................... 00:80:63:51:7A:80
Network Configuration Protocol (BootP/DHCP).... None
DHCP Client ID (same as SNMP System Name)..... "GCI-WS102"
Network Configuration Protocol HiDiscovery..... Read-Write
Management VLAN ID............................ 1
Management VLAN Priority...................... 7
Management IP-DSCP Value...................... 0(be/cs0)
Web Mode...................................... Enable
JavaScript Mode............................... Enable
```

FIGURE 103 – Layer 2 management priority

Configuring Layer 3 management priority

☐ Select the `QoS/Priority:Global` dialog.
☐ In the line `IP-DSCP value for management packets` enter the IP-DSCP value with which the Magnum 12KX sends management packets.

`enable`	**Switch to the Privileged EXEC mode.**
`network priority ip-dscp cs7`	**Assign the value cs7 to the management priority so that management packets with the highest priority are handled.**
`exit`	**Switch to the privileged EXEC mode.**
`show network`	**Displays the management VLAN priority.**

```
System IP Address............................. 10.0.1.116
Subnet Mask................................... 255.255.255.0
Default Gateway............................... 10.0.1.200
Burned In MAC Address......................... 00:80:63:51:7A:80
Network Configuration Protocol (BootP/DHCP).... None
DHCP Client ID (same as SNMP System Name)..... "PowerMICE-517A80"
Network Configuration Protocol HiDiscovery..... Read-Write
Management VLAN ID............................ 1
Management VLAN Priority...................... 7
Management IP-DSCP Value...................... 56(cs7)
Web Mode...................................... Enable
JavaScript Mode............................... Enable
```

FIGURE 104 – Layer 3 management priority

Chapter 10

Flow Control

Description of Flow Control

Flow control is a mechanism which acts as an overload protection for the Magnum 12KX. During periods of heavy traffic, it holds off additional traffic from the network.

The example below shows a graphic illustration of how the flow control works. Workstations 1, 2 and 3 want to simultaneously transmit a large amount of data to Workstation 4. The combined bandwidth of Workstations 1, 2 and 3 to the Magnum 12KX is larger than the bandwidth of Workstation 4 to the Magnum 12KX. This leads to an overflow of the send queue of port 4. The funnel on the left symbolizes this status.

If the flow control function at ports 1, 2 and 3 of the Magnum 12KX is turned on, the Magnum 12KX reacts before the funnel overflows. Ports 1, 2 and 3 send a message to the connected devices that no data can be received at present.

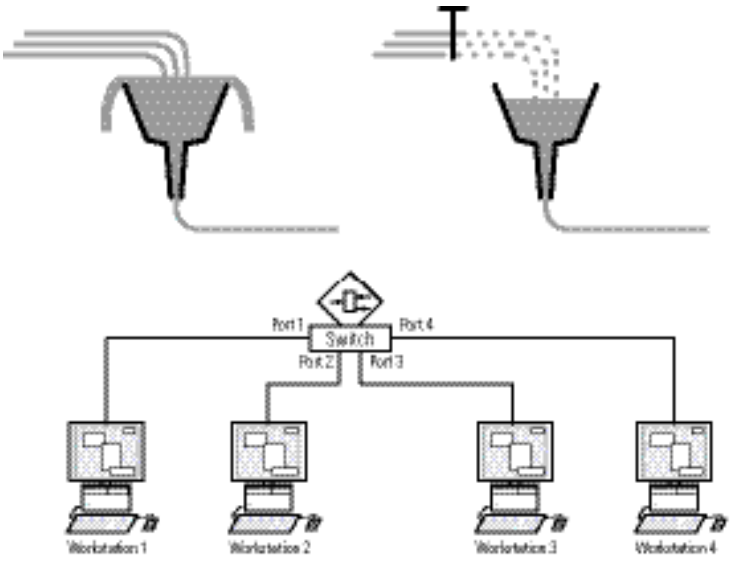


FIGURE 105 – Example of flow control

Flow Control with a full duplex link

In the example above there is a full duplex link between Workstation 2 and the Magnum 12KX. Before the send queue of port 2 overflows, the Magnum 12KX sends a request to Workstation 2 to include a small break in the sending transmission.

Note: The Magnum 12KX support flow control in full duplex mode only.

Flow Control with a half-duplex link

In the example above there is a half-duplex link between Workstation 2 and the Magnum 12KX. Before the send queue of port 2 overflows, the Magnum 12KX sends data back so that Workstation 2 detects a collision and interrupts the sending process.

Note: The Magnum 12KX does not support flow control in half duplex mode.

Setting the Flow Control

☐ Select the `Basics:Port Configuration` dialog.
In the "Flow Control on" column, checkmark this port to specify that flow control is active here. Also activate the global "Flow Control" switch in the `Switching:Global` dialog.

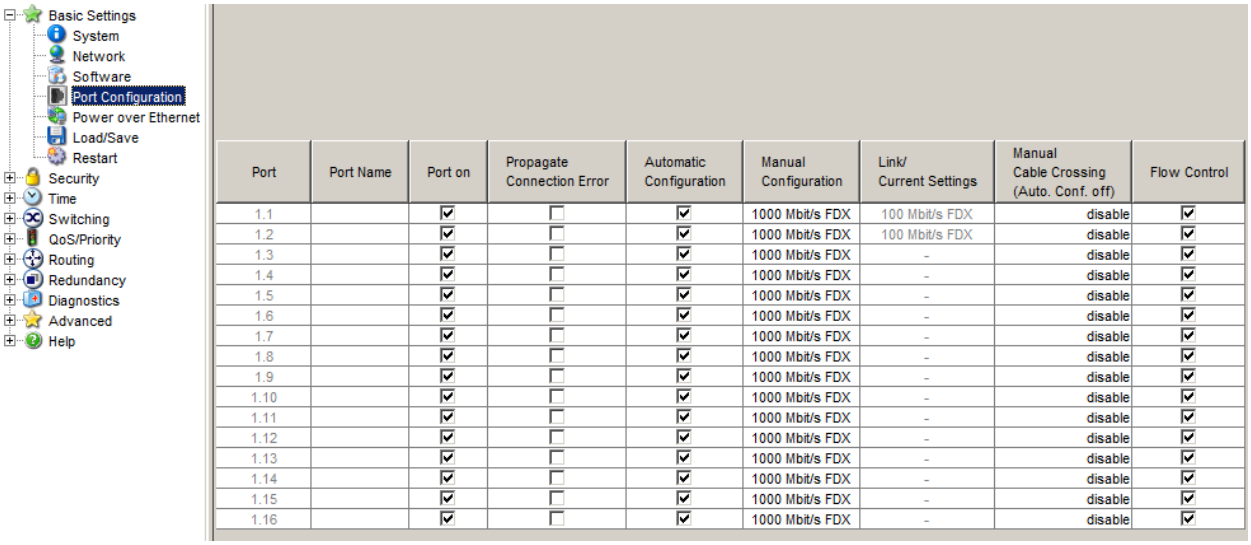


FIGURE 106 – Flow Control menus

☐ Select the `Switching:Global` dialog.

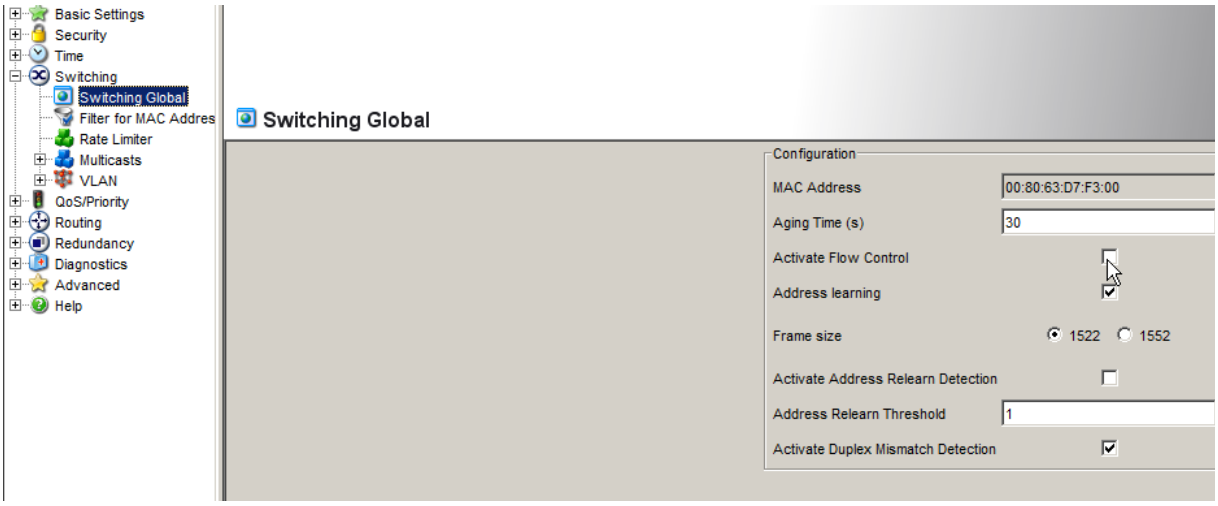


FIGURE 107 – Enabling Flow Control

With this dialog

- switch off the flow control at all ports or
- switch on the flow control at those ports for which the flow control is selected in the port configuration table.

Note: When using a redundancy function, deactivate the flow control on the participating ports. Default setting: flow control deactivated globally and activated on all ports.

If the flow control and the redundancy function are active at the same time, there is a risk of the redundancy failing.

Chapter 11

VLANs

VLAN Description

In the simplest case, a virtual LAN (VLAN) consists of a group of network participants in one network segment who can communicate with each other as if they belonged to a separate LAN.

More complex VLANs span out over multiple network segments and are also based on logical (instead of only physical) connections between network participants. Thus VLANs are an element of flexible network design, since the user can reconfigure logical connections centrally more easily than cable connections.

The IEEE 802.1Q standard defines the VLAN function.

The most important benefits of VLANs are:

- Network load limiting
  VLANs can reduce the network load considerably as a Switch only transmits Broadcast/Multicast data packets and Unicast packets with unknown (unlearned) destination addresses within the virtual LAN. The rest of the data network is unaffected by this.

- Flexibility
  Users have the option of forming user groups flexibly based on the function of the participants and not on their physical location or medium.

- Clarity
  VLANs give networks a clear structure and make maintenance easier.

Examples of VLANs

The following practical examples provide a quick introduction to the structure of a VLAN.

Example 1

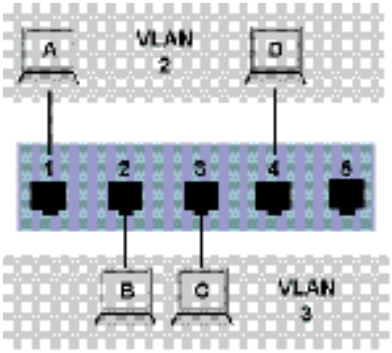


FIGURE 108 – Example of a simple port-based VLAN

The example shows a minimal VLAN configuration (port-based VLAN). An administrator has connected multiple terminal devices to a transmission device and assigned them to 2 VLANs. This effectively prohibits any data transmission between the VLANs, whose members communicate only within their own VLANs.
When setting up the VLANs, create communication rules for every port, by entering in incoming (ingress) and outgoing (egress) tables.
The ingress table specifies which VLAN ID a port assigns to the incoming data packets. Hereby, use the port address of the terminal device to assign it to a VLAN.
The egress table specifies to which VLAN the frames sent from this port are assigned. The entry also defines whether Ethernet frames sent from this port are to be tagged:

- T = with TAG field (T = tagged)
- U = without TAG field (U = untagged)

For the above example, the status of the TAG field of the data packets is not relevant, so it can generally be set to „U“.

Terminal	Port	Port	VLAN identifier (PVID)
A	1	2	
B	2	3	
C	3	3	
D	4	2	
	5	1	

Table 18: Ingress table

VLANID	Port				
	1	2	3	4	5
1					U
2	U			U	
3		U	U		

Table 19: Egress table

Proceed as follows to perform the example configuration:

☐ Configure VLAN

☐ Select the `Switching:VLAN:Static` dialog.

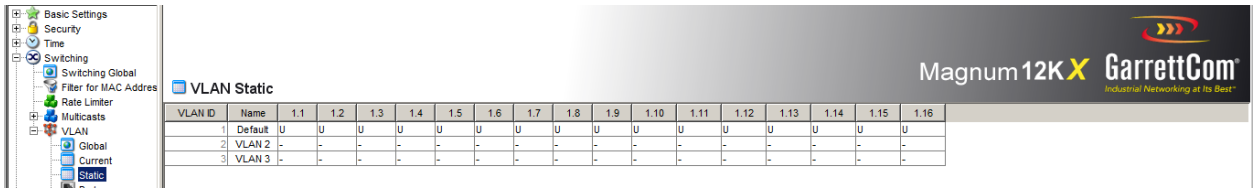


FIGURE 109 – Creating and naming new VLANs

☐ Click on “Create” to open a window for entering the VLAN ID.

☐ Assign VLAN ID 2 to the VLAN.

☐ Click on “OK”.

☐ Give this VLAN the name VLAN2 by clicking on the name field and entering the name. Also change the name for VLAN 1 from “Default” to “VLAN1”.

☐ Repeat the previous steps and create another VLAN with the VLAN ID 3 and the name VLAN3.

```
enable                      Switch to the Privileged EXEC mode.
vlan database               Switch to the VLAN configuration mode.
vlan 2                      Create a new VLAN with the VLAN ID 2.
vlan name 2 VLAN2           Give the VLAN with the VLAN ID 2 the name VLAN2.

vlan 3                      Create a new VLAN with the VLAN ID 3.
vlan name 3 VLAN3           Give the VLAN with the VLAN ID 3 the name VLAN3.

vlan name 1 VLAN1           Give the VLAN with the VLAN ID 1 the name VLAN1.

exit                        Leave the VLAN configuration mode.
show vlan brief             Display the current VLAN configuration.
Max. VLAN ID..................................... 4042
Max. supported VLANs.............................  255
Number of currently configured VLANs............    3
VLAN 0 Transparent Mode (Prio. Tagged Frames).. Disabled
VLAN ID VLAN Name                       VLAN Type VLAN Creation Time
---- -------------------------------- --------- ------------------
1       VLAN1                           Default    0 days, 00:00:05
2       VLAN2                           Static     0 days, 02:44:29
3       VLAN3                           Static     0 days, 02:52:26
```

FIGURE 110 – Setting VLANs using CLI

☐ Configuring the ports

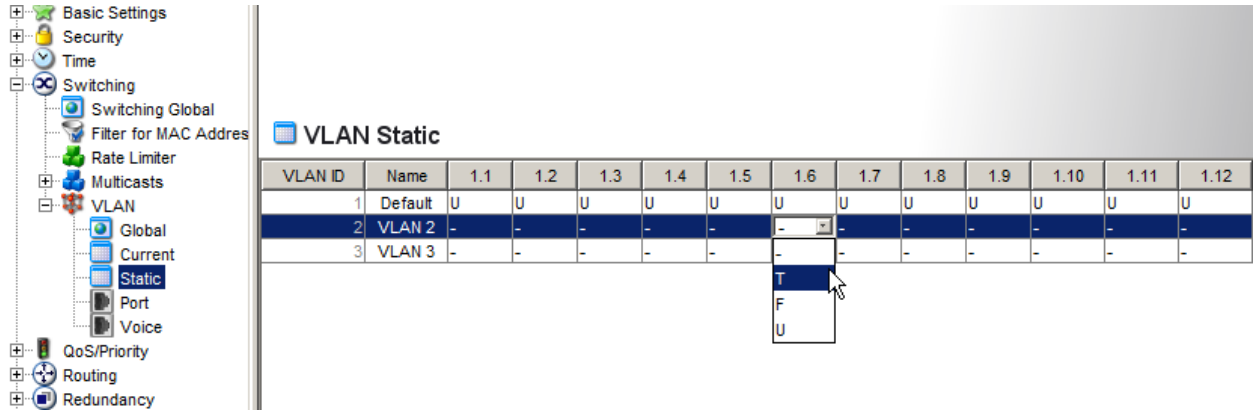


FIGURE 111 – Defining the VLAN membership of the ports.

☐ Assign the ports of the Magnum 12KX to the corresponding VLANs by clicking on the related table cell to open the selection menu and define the status. The selection options are:

- \- = currently not a member of this VLAN (GVRP allowed)
- T = member of VLAN; send data packets with tag
- U = Member of the VLAN; send data packets without tag
- F = not a member of the VLAN (also disabled for GVRP)

Because terminal devices usually do not interpret data packets with a tag, select the U setting here.

☐ Click “Set” to temporarily save the entry in the configuration.

☐ Select the `Switching:VLAN:Port` dialog.

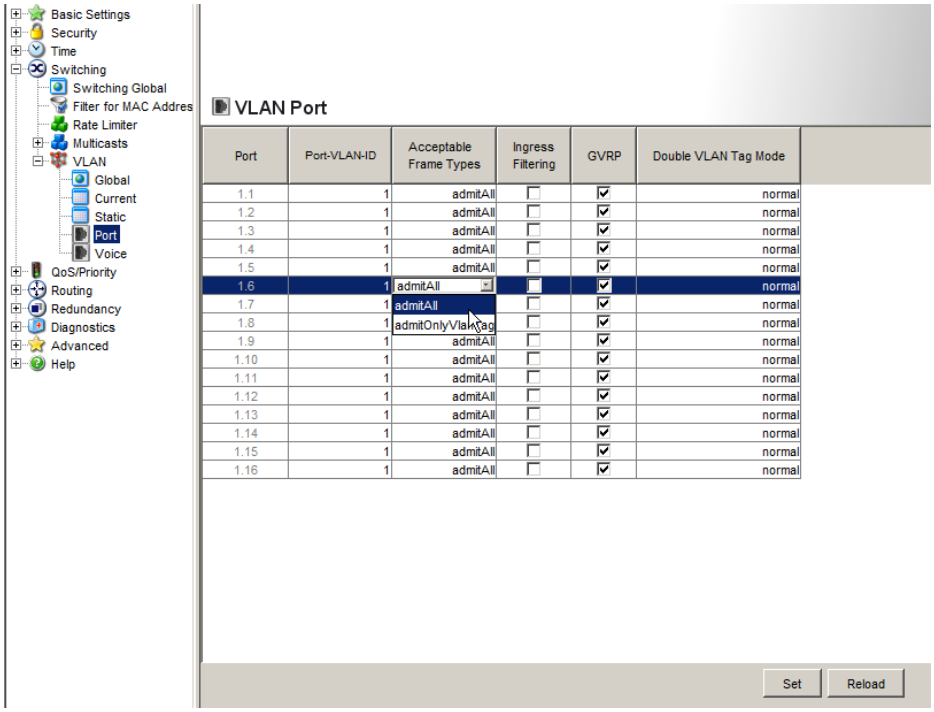


FIGURE 112 – Assign and save Port VLAN ID, Acceptable Frame Types and Ingress Filtering

☐ Assign the Port VLAN ID of the related VLANs (2 or 3) to the individual ports. See table.

☐ Because terminal devices usually do not send data packets with a tag, select the `admitAll` setting for "Acceptable Frame Types".

☐ The settings for `GVRP` and `Ingress Filter` do not affect how this example functions.

☐ Click "Set" to temporarily save the entry in the configuration.

☐ Select the `Basics: Load/Save` dialog.

☐ In the "Save" frame, select "To Device" for the location and click "Save" to permanently save the configuration in the active configuration.

`enable`	**Switch to the Privileged EXEC mode.**
`configure`	**Switch to the Configuration mode.**
`interface 1/1`	**Switch to the Interface Configuration mode of interface 1/1.**
`vlan participation include 2`	**Port 1/1 becomes member untagged in VLAN 2.**
`vlan pvid 2`	**Port 1/1 is assigned the port VLAN ID 2.**
`exit`	**Switch to the Configuration mode.**
`interface 1/2`	**Switch to the interface configuration mode for interface 1/2.**
`vlan participation include 3`	**Port 1/2 becomes member untagged in VLAN 3.**
`vlan pvid 3`	**Port 1/2 is assigned the port VLAN ID 3.**
`exit`	**Switch to the Configuration mode.**
`interface 1/3`	**Switch to the Interface Configuration mode of Interface 1/3.**
`vlan participation include 3`	**Port 1/3 becomes member untagged in VLAN 3.**
`vlan pvid 3`	**Port 1/3 is assigned the port VLAN ID 3.**
`exit`	**Switch to the Configuration mode.**
`interface 1/4`	**Switch to the interface configuration mode of interface 1/4.**
`vlan participation include 2`	**Port 1/4 becomes member untagged in VLAN 2.**
`vlan pvid 2`	**Port 1/4 is assigned the port VLAN ID 2.**
`exit`	**Switch to the Configuration mode.**
`exit`	**Switch to the privileged EXEC mode.**
`show VLAN 3`	**Show details for VLAN 3.**

```
VLAN ID           : 3
VLAN Name         : VLAN3
VLAN Type         : Static
VLAN Creation Time: 0 days, 02:52:26 (System Uptime)
Interface   Current   Configured   Tagging
----------  --------  -----------  --------
1/1         Exclude   Autodetect   Tagged
1/2         Include   Include      Untagged
1/3         Include   Include      Untagged
1/4         Exclude   Autodetect   Tagged
1/5         Exclude   Autodetect   Tagged
```

FIGURE 113 – Assigning VLANs to an interface

Example 2

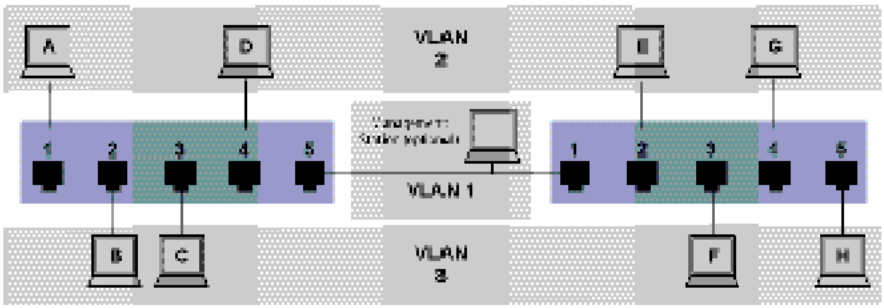


FIGURE 114 – Example of a more complex VLAN constellation

The second example shows a more complex constellation with 3 VLANs (1 to 3). Along with the Switch from example 1, a second Switch (on the right in the example) is now used.
The terminal devices of the individual VLANs (A to H) are spread over two transmission devices (Switches). Such VLANs are therefore known as distributed VLANs. An optional Management Station is also shown, which enables access to all network components if it is configured correctly.

Note: In this case, VLAN 1 has no significance for the terminal device communication, but it is required to maintain the administration of the transmission devices via what is known as the Management VLAN.

As in the previous example, uniquely assign the ports with their connected terminal devices to a VLAN. With the direct connection between the two transmission devices (uplink), the ports transport packets for both VLANs. To differentiate these, “VLAN tagging” is used, which prepares the packets accordingly. This maintains the respective VLAN assignments.

Proceed as follows to perform the example configuration:
Add Uplink Port 5 to the ingress and egress tables from example 1. Create new ingress and egress tables for the right switch, as described in the first example.
The egress table specifies to which VLAN the frames sent from this port are assigned. The entry also defines whether Ethernet frames sent from this port are to be tagged:

- T = with TAG field (T = tagged)
- U = without TAG field (U = untagged)

In this example, tagged frames are used in the communication between the transmission devices (uplink), as frames for different VLANs are differentiated at these ports.

Terminal	Port	Port	VLAN identifier (PVID)
A	1	2	
B	2	3	
C	3	3	
D	4	2	
Uplink	5	1	

Table 20: Ingress table for device on left

Terminal	Port	Port	VLAN identifier (PVID)
Uplink	1	1	
E	2	2	
F	3	3	
G	4	2	
H	5	3	

Table 21: Ingress table for device on right

VLAN ID	Port				
	1	2	3	4	5
1					U
2	U			U	T
3		U	U		T

Table 22: Egress table for device on left

VLAN ID	Port				
	1	2	3	4	5
1	U				
2	T	U		U	
3	T		U		U

Table 23: Egress table for device on right

The communication relationships here are as follows: terminal devices at ports 1 and 4 of the left device and terminal devices at ports 2 and 4 of the right device are members of VLAN 2 and can thus communicate with each other. The behavior is the same for the terminal devices at ports 2 and 3 of the left device and the terminal devices at ports 3 and 5 of the right device. These belong to VLAN 3.

The terminal devices “see” their respective part of the network and cannot reach any other participant outside their VLAN. Broadcast and Multicast data packets, and Unicast packets with unknown (unlearned) target addresses as also only sent within a VLAN.

Here, VLAN tagging (IEEE 801.1Q) is used within the VLAN with the ID 1 (Uplink). This is denoted by the letters (T) in the egress table of the ports.

The configuration of the example is the same for the device on the right. Proceed in the same way, using the ingress and egress tables created above to adapt the previously configured left device to the new environment.

Proceed as follows to perform the example configuration:

☐ Configure VLAN

☐ Select the `Switching:VLAN:Static` dialog.

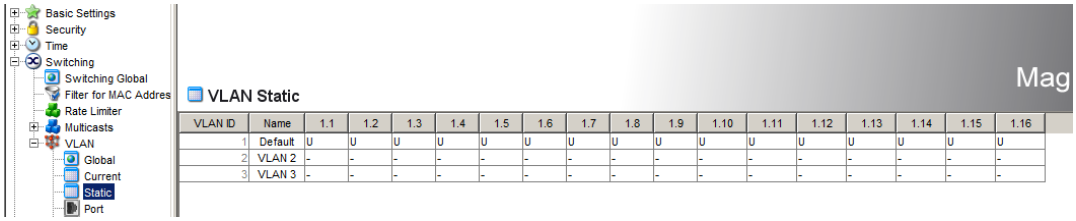


FIGURE 115 – Creating and naming new VLANs

☐ Click on “Create” to open a window for entering the VLAN ID.

☐ Assign VLAN ID 2 to the VLAN.

☐ Give this VLAN the name VLAN2 by clicking on the name field and entering the name. Also change the name for VLAN 1 from “Default” to “VLAN1”.

☐ Repeat the previous steps and create another VLAN with the VLAN ID 3 and the name “VLAN3”.

`enable`	**Switch to the Privileged EXEC mode.**
`vlan database`	**Switch to the VLAN configuration mode.**
`vlan 2`	**Create a new VLAN with the VLAN ID 2.**
`vlan name 2 VLAN2`	**Give the VLAN with the VLAN ID 2 the name VLAN2.**
`vlan 3`	**Create a new VLAN with the VLAN ID 3.**
`vlan name 3 VLAN3`	**Give the VLAN with the VLAN ID 3 the name VLAN3.**
`vlan name 1 VLAN1`	**Give the VLAN with the VLAN ID 1 the name VLAN1.**
`exit`	**Switch to the privileged EXEC mode.**
`show vlan brief`	**Display the current VLAN configuration.**

```
Max. VLAN ID..................................... 4042
Max. supported VLANs............................   255
Number of currently configured VLANs...........     3
VLAN 0 Transparent Mode (Prio. Tagged Frames).. Disabled
VLAN ID VLAN Name                       VLAN Type VLAN Creation Time
---- -------------------------------- --------- ------------------
1       VLAN1                           Default    0 days, 00:00:05
2       VLAN2                           Static     0 days, 02:44:29
3       VLAN3                           Static     0 days, 02:52:26
```

FIGURE 116 – Setting VLANs using CLI

☐ Configuring the ports

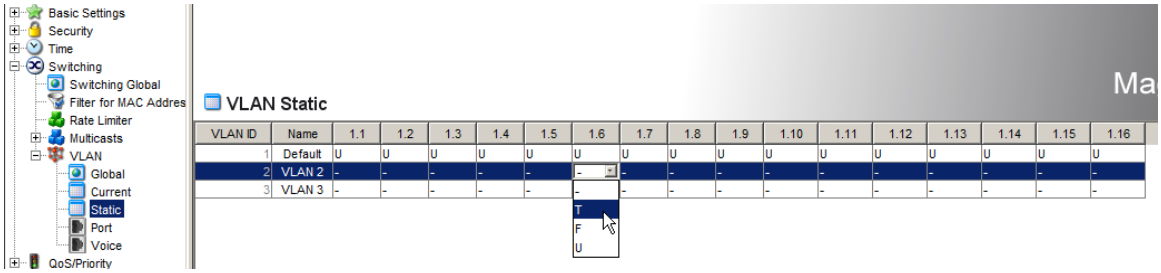


FIGURE 117 – Defining the VLAN membership of the ports.

☐ Assign the ports of the Magnum 12KX to the corresponding VLANs by clicking on the related table cell to open the selection menu and define the status. The selection options are:

- \- = currently not a member of this VLAN (GVRP allowed)
- T = member of VLAN; send data packets with tag
- U = Member of the VLAN; send data packets without tag
- F = not a member of the VLAN (also disabled for GVRP)

Because terminal devices usually do not interpret data packets with a tag, select the U setting. Only select the T setting at the uplink port at which the VLANs communicate with each other.

☐ Click “Set” to temporarily save the entry in the configuration.

☐ Select the `Switching:VLAN:Port` dialog.

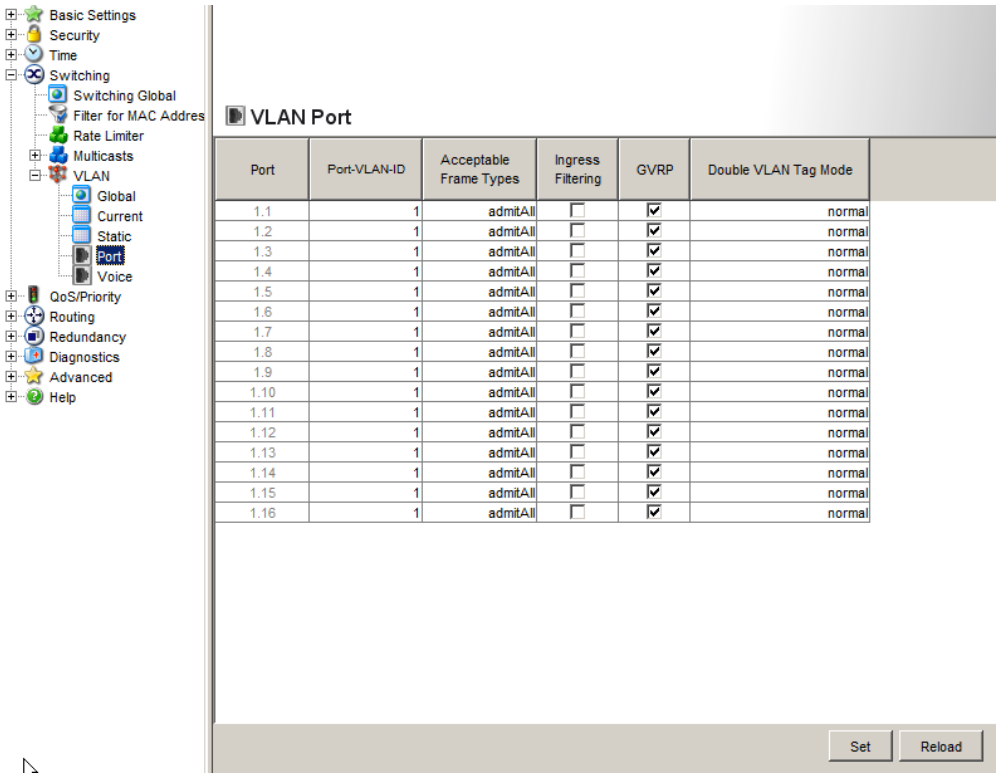


FIGURE 118 – Assign and save Port VLAN ID, Acceptable Frame Types and Ingress Filtering

☐ Assign the ID of the related VLANs (1 to 3) to the individual ports.

☐ Because terminal devices usually do not send data packets with a tag, select the `admitAll` setting for the terminal device ports. Configure the uplink port with `admit only VLAN tags.`

☐ Activate `Ingress Filtering` at the uplink port so that the VLAN tag is evaluated at this port.

☐ Click “Set” to temporarily save the entry in the configuration.

☐ Select the `Basics: Load/Save` dialog.

☐ In the “Save” frame, select “To Device” for the location and click “Save” to permanently save the configuration in the active configuration.

`enable`	**Switch to the Privileged EXEC mode.**
`configure`	**Switch to the Configuration mode.**
`interface 1/1`	**Switch to the Interface Configuration mode of interface 1/1.**
`vlan participation include 1`	**Port 1/1 becomes member untagged in VLAN 1.**
`vlan participation include 2`	**Port 1/1 becomes member untagged in VLAN 2.**
`vlan tagging 2`	**Port 1/1 becomes member tagged in VLAN 2.**
`vlan participation`	**Port 1/1 becomes member untagged in VLAN 3.**

```
include 3
vlan tagging 3          Port 1/1 becomes member tagged in VLAN 3.
vlan pvid 1             Port 1/1 is assigned the port VLAN ID 1.
vlan ingressfilter      Port 1/1 ingress filtering is activated.
vlan acceptframe        Port 1/1 only forwards frames with a VLAN tag.
vlanonly
exit                    Switch to the Configuration mode.
interface 1/2           Switch to the interface configuration mode for interface 1/2.

vlan participation      Port 1/2 becomes member untagged in VLAN 2.
include 2
vlan pvid 2             Port 1/2 is assigned the port VLAN ID 2.
exit                    Switch to the Configuration mode.
interface 1/3           Switch to the Interface Configuration mode of Interface 1/3.

vlan participation      Port 1/3 becomes member untagged in VLAN 3.
include 3
vlan pvid 3             Port 1/3 is assigned the port VLAN ID 3.
exit                    Switch to the Configuration mode.
interface 1/4           Switch to the interface configuration mode of interface 1/4.

vlan participation      Port 1/4 becomes member untagged in VLAN 2.
include 2
vlan pvid 2             Port 1/4 is assigned the port VLAN ID 2.
exit                    Switch to the Configuration mode.
interface 1/5           Switch to the interface configuration mode for port 1.5.

vlan participation      Port 1/5 becomes member untagged in VLAN 3.
include 3
vlan pvid 3             Port 1/5 is assigned the port VLAN ID 3.
exit                    Switch to the Configuration mode.
exit                    Switch to the privileged EXEC mode.
show vlan 3             Show details for VLAN 3.
VLAN ID           : 3
VLAN Name         : VLAN3
VLAN Type         : Static
VLAN Creation Time: 0 days, 00:07:47 (System Uptime)
Interface   Current   Configured   Tagging
----------  --------  -----------  --------
1/1         Include   Include      Tagged
1/2         Exclude   Autodetect   Untagged
1/3         Include   Include      Untagged
1/4         Exclude   Autodetect   Untagged
1/5         Include   Include      Untagged
```

FIGURE 119 – Setting multiple VLANs on an interface using CLI

For further information on VLANs, see the integrated help function in the program.

Chapter 12

Operation Diagnostics

Diagnostic Tools

The Magnum 12KX provides the following diagnostic tools:

- Sending traps
- Monitoring the Magnum 12KX status
- Out-of-band signaling via signal contact
- Port status indication
- Event counter at port level
- Detecting non-matching duplex modes
- SFP status display
- TP cable diagnosis
- Topology Discovery
- Detecting IP address conflicts
- Detecting loops
- Reports
- Monitoring data traffic at a port (port mirroring)
- Syslog
- Event log

Sending Traps

If unusual events occur during normal operation of the Magnum 12KX, they are reported immediately to the management station. This is done by means of what are called traps i.e. alarm messages that bypass the polling procedure ("Polling" means querying the data stations at regular intervals). Traps make it possible to react quickly to critical situations.

Examples of such events are:

- a hardware reset
- changes to the configuration
- segmentation of a port

etc.

Traps can be sent to various hosts to increase the transmission reliability for the messages. A trap message consists of a packet that is not acknowledged. The Magnum 12KX sends traps to those hosts that are entered in the trap destination table. The trap destination table can be configured with the management station via SNMP.

List of SNMP Traps

All the possible traps that the Magnum 12KX can send are listed in the following table.

Trap name	Meaning
authenticationFailure	is sent if a station attempts to access the agent without permission.
coldStart	is sent for both cold and warm starts during the boot process after successful management initialization.
hmAutoconfigAdapterTrap	is sent when AutoConfiguration AdapterACA is removed or plugged in.
linkDown	is sent if the link to a port is interrupted.
linkUp	is sent as soon as the link to a port is re-established.
hmTemperature	is sent if the temperature exceeds the set threshold values.
hmPowerSupply	is sent if the status of the voltage supply changes.
hmSigConRelayChange	is sent if the status of the signal contact changes during the operation monitoring.
newRoot	is sent if the sending agent becomes the new root of the spanning tree.
topologyChange	is sent if the transmission mode of a port changes.
risingAlarm	is sent if an RMON alarm input exceeds the upper threshold.
fallingAlarm	is sent if an RMON alarm input falls below the lower threshold.
hmPortSecurityTrap	is sent if a MAC/IP address is detected at the port which does not correspond to the current settings of: – hmPortSecPermission and – hmPorSecAction is set to either trapOnly (2) or portDisable (3).
hmModuleMapChange	is sent if the hardware configuration is changed.
hmBPDUGuardTrap	is sent if a BPDU is received at a port when the BPDU Guard function is active.
hmMrpReconfig	is sent if the configuration of the MRP-Ring changes.
hmRingRedReconfig	is sent if the configuration of the HIPER-Ring changes.
hmRingRedCplReconfig	is sent if the configuration of the redundant ring/network coupling changes.
hmSNTPTrap	is sent if errors occur in connection with the SNTP (e.g. server cannot be reached).
hmRelayDuplicateTrap	is sent if a duplicate IP address is detected in connection with DHCP Option 82.
lldpRemTablesChangeTrap	is sent if an entry in the topology remote table is changed.
vrrpTrapNewMaster	is sent if a different router becomes the master for an interface or a virtual address.
vrrpTrapAuthFailure	is sent if the router receives a packet with invalid authentication from another VRRP router.
hmConfiguration-SavedTrap	is sent after the Magnum 12KX has successfully saved its configuration locally.
hmConfiguration-ChangedTrap	is sent when the configuration of the Magnum 12KX is changed for the first time after it has been saved locally.
hmAddressRelearnDetectTrap	is sent when Address Relearn Detection is activated and the threshold for the MAC addresses relearned at different ports has been exceeded. This process very probably indicates a loop situation in the network.

hmDuplexMismatchTrap	is sent if the Magnum 12KX has detected a potential problem with the duplex mode of a port.

Table 24: Possible traps

SNMP Traps during Boot

The Magnum 12KX sends the ColdStart trap every time it boots.

Configuring Traps

☐ Select the `Diagnostics:Alarms (Traps)` dialog.

This dialog allows the user to determine which events trigger an alarm (trap) and where these alarms should be sent.

☐ Select “Create entry”.
☐ In the “IP Address” column, enter the IP address of the recipient to whom the traps should be sent.
☐ In the “Active” column, select the entries which should be taken into account when traps are being sent.
☐ In the “Selection” frame, select the trap categories from which traps need to be sent.

Note: Read-write access is needed for this dialog.

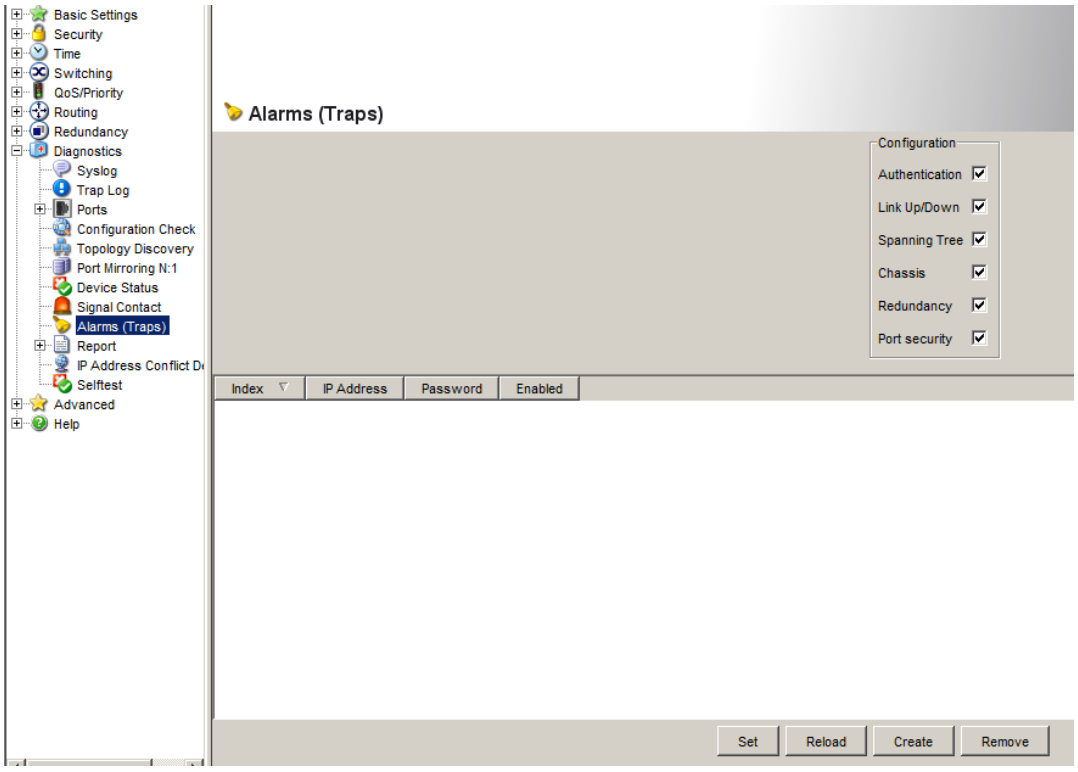


FIGURE 120 – Alarms dialog

The events which can be selected are:

Name	Meaning
Authentication	The Magnum 12KX has rejected an unauthorized access attempt (see the `Access for IP Addresses and Port Security` dialog).
Link Up/Down	At one port of the Magnum 12KX, the link to another device has been established/interrupted.
Spanning Tree	The topology of the Rapid Spanning Tree has changed.
Chassis	Summarizes the following events: – The status of a supply voltage has changed (see the System dialog). – The status of the signal contact has changed. To take this event into account, activate “Create trap when status changes” in the `Diagnostics:Signal Contact 1/2` dialog. – A media module has been added or removed (only for modular devices). – The AutoConfiguration Adapter (ACA) was added or removed. – The configuration on the AutoConfiguration Adapter (ACA) does not match that of the device. – The temperature thresholds were not met or were exceeded. – The receiver power status of a port with an SFP module has changed (see dialog `Dialog:Ports:SFP Modules`). – The configuration has been successfully saved in the Magnum 12KX and in the AutoConfiguration Adapter(ACA), if present. – The configuration has been changed for the first time after being saved in the device.
Redundancy	The redundancy status of the ring redundancy (redundant line active/inactive) or (for devices that support redundant ring/network coupling) the redundant ring/network coupling (redundancy exists) has changed.
Port security	On one port a data packet has been received from an unauthorized terminal device (see the `Port Security` dialog).

Table 25: Trap categories

Monitoring the Magnum 12KX Status

The Magnum 12KX status provides an overview of the overall condition of the device. Many process visualization systems record the device status in order to present its condition in graphic form.
The Magnum 12KX enables user to

- signal the device status out-of-band via a signal contact
- signal the device status by sending a trap when the device status changes
- detect the device status in the Web-based interface on the system side.
- query the device status in the Command Line Interface.

The device status of the device includes:

- Incorrect supply voltage,
  at least one of the two supply voltages is inoperative,
  the internal supply voltage is inoperative.
- The temperature threshold has been exceeded or has not been reached.
- The removal of a module (for modular devices).
- The removal of the ACA.
- The configuration on the ACA does not match that in the device.
- The interruption of the connection at at least one port. In the `Basic Settings:Port Configuration` menu, define which ports the device signals if the connection is down. By default, there is no link monitoring.
- Event in the ring redundancy:
  Loss of the redundancy (in ring manager mode). By default, there is no ring redundancy monitoring.
- Event in the ring/network coupling:
  Loss of the redundancy. By default, there is no ring redundancy monitoring.
  The following conditions are also reported by the device in standby mode:
  – Defective link status of the control line
  – Partner device is in standby mode
- Failure of a fan (MACH 4000).

Select the corresponding entries to decide which events the device status includes.

Note: With a non-redundant voltage supply, the Magnum 12KX reports the absence of a supply voltage. If the user does not want this message to be displayed, feed the supply voltage over both inputs or switch off the monitoring.

Configuring the Magnum 12KX Status

- ☐ Select the `Diagnostics:Device Status` dialog.
- ☐ In the "Monitoring" field, select the events that need to be monitored.
- ☐ To monitor the temperature, set the temperature thresholds in the `Basics:System` dialog at the end of the system data.

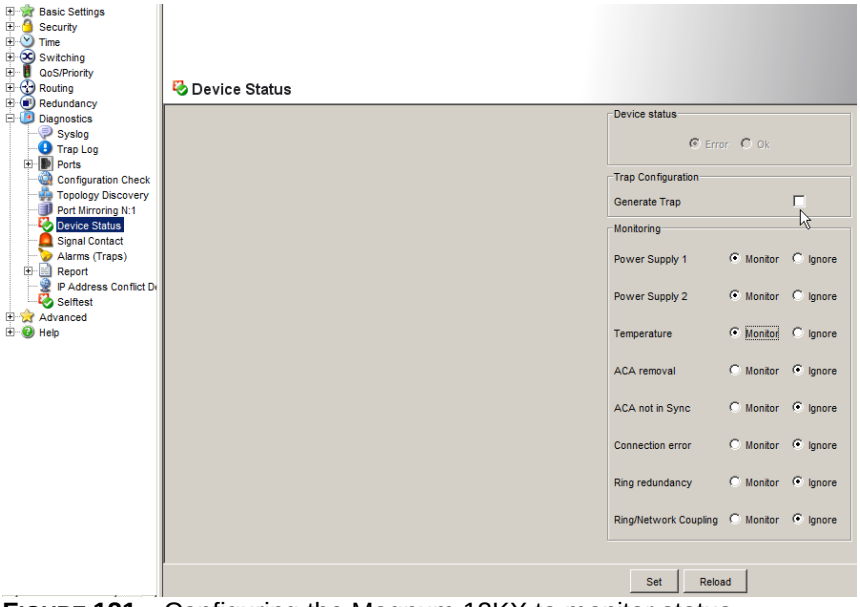


FIGURE 121 – Configuring the Magnum 12KX to monitor status

`enable`	**Switch to the Privileged EXEC mode.**
`configure`	**Switch to the Configuration mode.**
`device-status monitor all error`	**Include all the possible events in the device status determination.**
`device-status trap enable`	**Enable a trap to be sent if the device status changes.**

FIGURE 122 – Setting Magnum 12KX status monitoring

Note: The above CLI commands activate the monitoring and the trapping respectively for all the supported components. If monitoring needs to be activated or deactivated only for individual components, the corresponding syntax can be found in the CLI manual or in the help (Input ?) of the CLI console.

Displaying the Magnum 12KX Status

☐ Select the `Basics:System` dialog.

Magnum 12KX status and alarm display
1 - The symbol displays the Magnum 12KX status
2 - Cause of the oldest existing alarm
3 - Start of the oldest existing alarm

FIGURE 123 – Magnum 12KX Status

`exit`	**Switch to the privileged EXEC mode.**
`show device-status`	**Display the Magnum 12KX status and the setting for the device status determination.**

FIGURE 124 – Display Magnum 12KX status using CLI

Out-of-band Signaling

The signal contact is used to control external devices and monitor the operation of the Magnum 12KX. Function monitoring enables the user to perform remote diagnostics.
The Magnum 12KX reports the operating status via a break in the potential-free signal contact (relay contact, closed circuit):

- Incorrect supply voltage,
  at least one of the two supply voltages is inoperative,
  the internal supply voltage is inoperative.
- The temperature threshold has been exceeded or has not been reached.
- The removal of a module (for modular devices).
- The removal of the ACA.
- The configuration on the ACA does not match that in the device.
- The interruption of the connection at at least one port. In the `Basic Settings:Port Configuration` menu, define which ports the Magnum 12KX signals if the connection is down. By default, there is no link monitoring.
- Event in the ring redundancy:
  Loss of the redundancy (in ring manager mode). By default, there is no ring redundancy monitoring.
- Event in the ring/network coupling:
  Loss of the redundancy. By default, there is no ring redundancy monitoring.
  The following conditions are also reported by the Magnum 12KX in standby mode:
  – Defective link status of the control line
  – Partner device is in standby mode
- Failure of a fan (MACH 4000).

Select the corresponding entries to decide which events the Magnum 12KX status includes.

Note: With a non-redundant voltage supply, the Magnum 12KX reports the absence of a supply voltage. If the user does not want this message to be displayed, feed the supply voltage over both inputs or switch off the monitoring.

Controlling the Signal Contact

With this mode the user can remotely control every signal contact individually.

Application options:

- Simulation of an error as an input for process control monitoring equipment.
- Remote control of a Magnum 12KX via SNMP, such as switching on a camera.

☐ Select the `Diagnostics:Signal Contact 1/2)` dialog.

☐ In the "Mode Signal contact" frame, select the "Manual setting" mode to switch the contact manually.

☐ Select "Opened" in the "Manual setting" frame to open the contact.

☐ Select "Closed" in the "Manual setting" frame to close the contact.

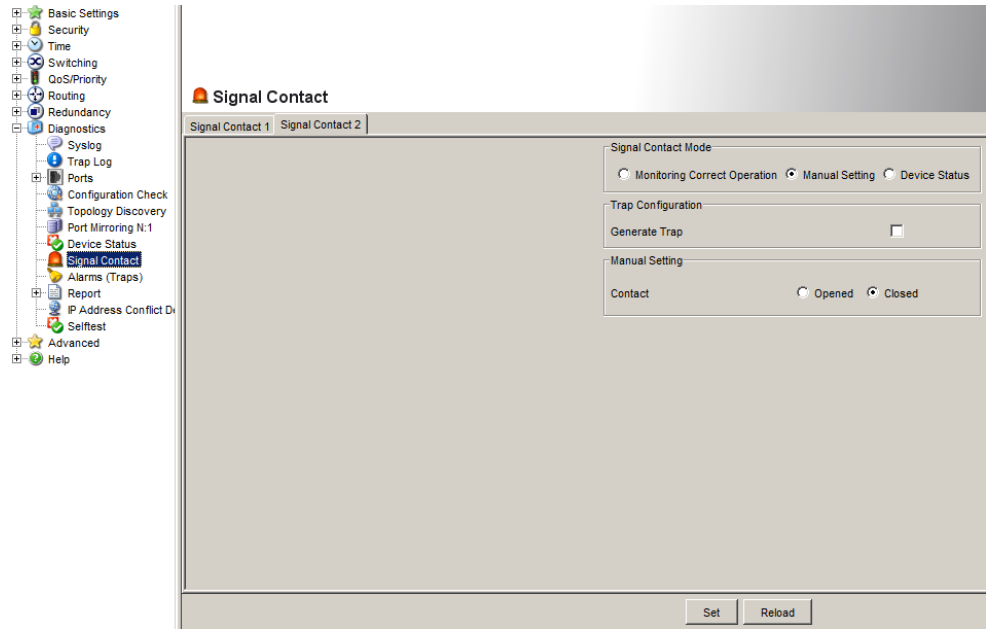


FIGURE 125 – Configuring Signal Contact

`enable`	**Switch to the Privileged EXEC mode.**
`configure`	**Switch to the Configuration mode.**
`signal-contact 1 mode manual`	**Select the manual setting mode for signal contact 1.**
`signal-contact 1 state open`	**Open signal contact 1.**
`signal-contact 1 state closed`	**Close signal contact 1.**

FIGURE 126 – Configuring Signal Contact using CLI

Monitoring the Magnum 12KX Status via the Signal Contact

The "Device Status" option enables the user (like in the operation monitoring) to monitor the Magnum 12KX state via the signal contact.

Monitoring the Magnum 12KX Functions via the Signal Contact

Configuring the operation monitoring

- ☐ Select the `Diagnostics:Signal Contact` dialog.
- ☐ Select "Monitoring correct operation" in the "Mode signal contact" frame to use the contact for operation monitoring.
- ☐ In the "Monitoring correct operation" frame, select the events that need monitoring.
- ☐ To monitor the temperature, set the temperature thresholds in the `Basics:System` dialog at the end of the system data.

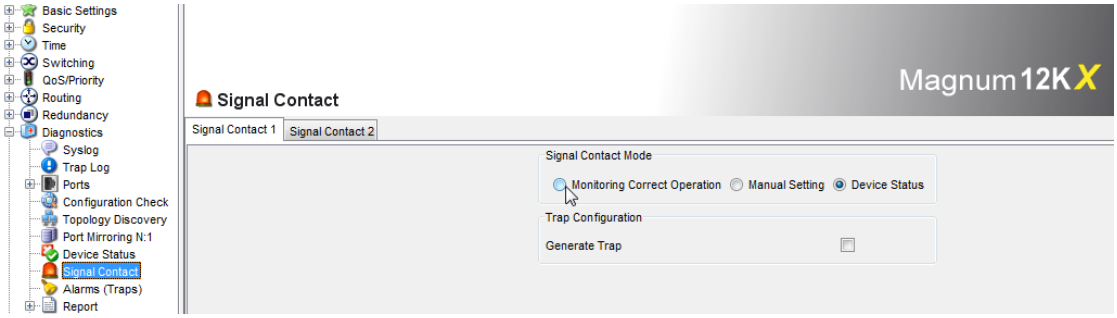


FIGURE 127 – Monitoring Signal Contact

`enable`	**Switch to the Privileged EXEC mode.**
`configure`	**Switch to the Configuration mode.**
`signal-contact 1 monitor all`	**Includes all the possible events in the operation monitoring.**
`signal-contact 1 trap enable`	**Enables a trap to be sent if the status of the operation monitoring changes.**

FIGURE 128 – Monitoring Signal Contact using CLI

Displaying the signal contact's status

The Magnum 12KX gives 3 additional options for displaying the status of the signal contact:

- LED display on Magnum 12KX,
- Display in the Web-based interface,
- Query in the Command Line Interface.

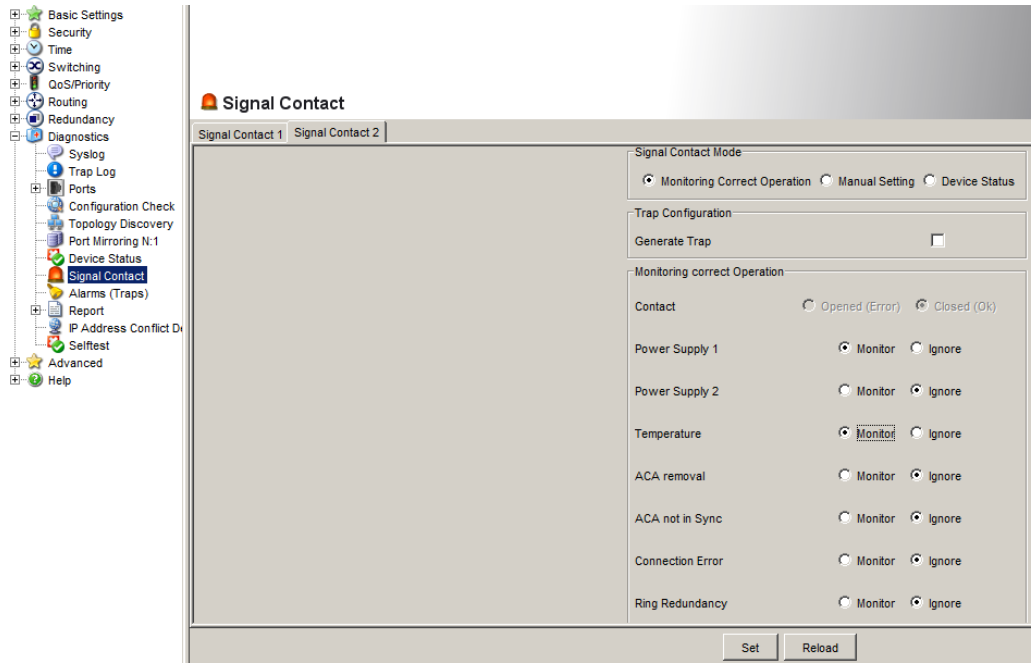


FIGURE 129 – Signal Contact dialog

`exit`	**Switch to the privileged EXEC mode.**
`show signal-contact 1`	**Displays the status of the operation monitoring and the setting for the status determination.**

FIGURE 130 – Displaying Signal Contact using CLI

Monitoring the Fan

Fans are subject to natural wear. The failure of one or more fans in the plug-in fan can have a negative effect on the operation and life span of the Magnum 12KX, or can lead to a total failure of the device.

The Magnum 12KX enables the user

- To signal changes to the status of the plug-in fan out-of-band (outside the data flow) via a signal contact.
- To signal changes to the status of the plug-in fan by sending a trap when the Magnum 12KX status changes
- To detect status changes to the plug-in fan in the Web-based interface on the system side and
- To query changes to the status of the plug-in fan in the Command Line Interface.

Proceed as follows to signal changes to the fan status via a signal contact and with an alarm message:

- ☐ Select the `Diagnostics:Signal Contact` dialog.
- ☐ Select the signal contact needed to use (in the example, signal contact 1) in the corresponding tab page “Signal contact 1” or “Signal contact 2”. (See figure above).
- ☐ In the “Signal contact mode” frame, select “Function monitoring”.
- ☐ In the “Function monitoring” frame, select the fan monitoring.
- ☐ Click “Set” to temporarily save the entry in the configuration.
- ☐ Select the `Basics: Load/Save` dialog.
- ☐ In the “Save” frame, select “To Device” for the location and click “Save” to permanently save the configuration in the active configuration.

Port Status Indication

- ☐ Select the `Basics:System` dialog.

The device view shows the device with the current configuration. The symbols underneath the device view represent the status of the individual ports.

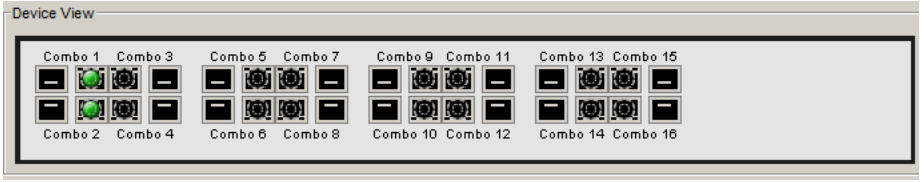


FIGURE 131 – Device View

Meaning of the symbols:

 The port (10, 100 Mbit/s, 1, 10 Gbit/s) is enabled and the connection is OK.

 The port is disabled by the management and it has a connection.

 The port is disabled by the management and it has no connection.

The port is in autonegotiation mode.

The port is in HDX mode.

The port is in RSTP discarding mode (100 Mbit/s).

The port is in routing mode (100 Mbit/s).

Event Counter at Port Level

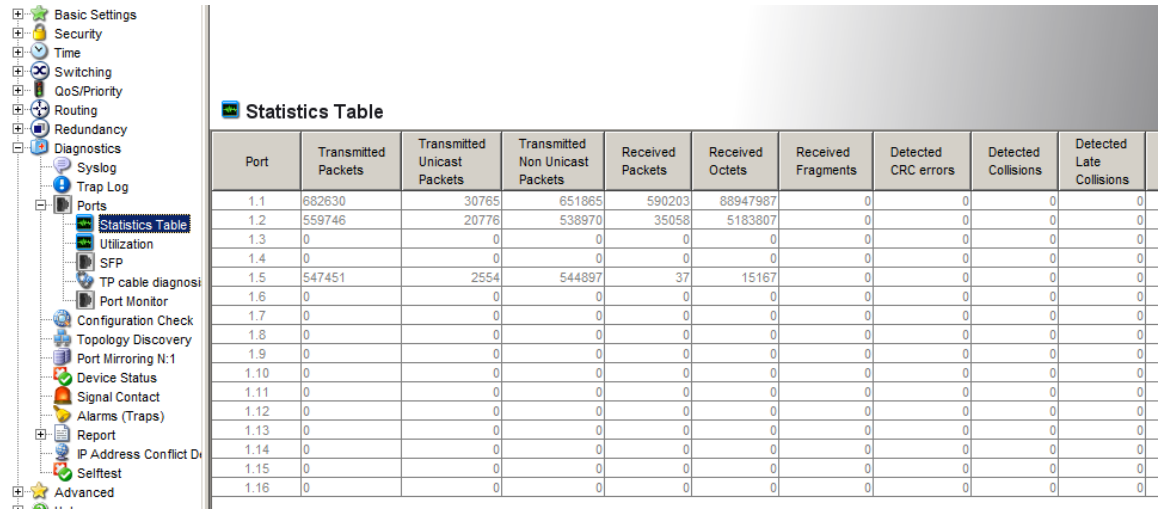
The port statistics table enables experienced network administrators to identify possible detected problems in the network.
This table shows the contents of various event counters. In the Restart menu item, reset all the event counters to zero using "Warm start", "Cold start" or "Reset port counter".
The packet counters add up the events sent and the events received.

Counter	Possible detected problem
Received fragments	– The controller of the connected device is inoperable – Electromagnetic interference in the transmission medium
CRC error	– The controller of the connected device is inoperable – Electromagnetic interference in the transmission medium – Defective component in the network
Collisions	– The controller of the connected device is inoperable – Network overextended/lines too long – Collision of a fault with a data packet

Table 26: Examples indicating possible detected problems

☐ Select the `Diagnostics:Ports:Statistics Table` dialog.

☐ To reset the counters, click on "Reset port counters" in the Basics:Restart dialog.



Port	Transmitted Packets	Transmitted Unicast Packets	Transmitted Non Unicast Packets	Received Packets	Received Octets	Received Fragments	Detected CRC errors	Detected Collisions	Detected Late Collisions
1.1	682630	30765	651865	590203	88947987	0	0	0	0
1.2	559746	20776	538970	35058	5183807	0	0	0	0
1.3	0	0	0	0	0	0	0	0	0
1.4	0	0	0	0	0	0	0	0	0
1.5	547451	2554	544897	37	15167	0	0	0	0
1.6	0	0	0	0	0	0	0	0	0
1.7	0	0	0	0	0	0	0	0	0
1.8	0	0	0	0	0	0	0	0	0
1.9	0	0	0	0	0	0	0	0	0
1.10	0	0	0	0	0	0	0	0	0
1.11	0	0	0	0	0	0	0	0	0
1.12	0	0	0	0	0	0	0	0	0
1.13	0	0	0	0	0	0	0	0	0
1.14	0	0	0	0	0	0	0	0	0
1.15	0	0	0	0	0	0	0	0	0
1.16	0	0	0	0	0	0	0	0	0

FIGURE 132 – Device Port Statistics

Detecting Non-matching Duplex Modes

If the duplex modes of 2 ports directly connected to each other do not match, this can cause problems that are difficult to track down. The automatic detection and reporting of this situation has the benefit of recognizing it before problems occur.

This situation can arise from an incorrect configuration, e.g. if the automatic configuration is deactivated at the remote port.

A typical effect of this non-matching is that at a low data rate, the connection seems to be functioning, but at a higher bi-directional traffic level the local device records a lot of CRC errors, and the connection falls significantly below its nominal capacity.

The Magnum 12KX allows the user to detect this situation and report it to the network management station. In the process, the Magnum 12KX evaluates the error counters of the port in the context of the port settings.

Possible Causes of Port Error Events

The following table lists the duplex operating modes for TX ports together with the possible error events. The terms in the table mean:

- Collisions: In half-duplex mode, collisions mean normal operation.
- Duplex problem: Duplex modes do not match.
- EMI: Electromagnetic interference.
- Network extension: The network extension too great, or too many hubs are cascaded.
- Collisions, late collisions: In full-duplex mode, the port does not count collisions or late collisions.
- CRC error: The Magnum 12KX only evaluates these errors as duplex problems in the manual full duplex mode.

No.	Auto-negotiation	Current duplex mode	Detected error events (≥ 10)	Evaluation of duplex situation by device	Possible causes
1	On	Half duplex	None	OK	

2	On	Half duplex	Collisions	OK	
3	On	Half duplex	Late collisions	Duplex problem detected	Duplex problem, EMI, network extension
4	On	Half duplex	CRC error	OK	EMI
5	On	Full duplex	None	OK	
6	On	Full duplex	Collisions	OK	EMI
7	On	Full duplex	Late collisions	OK	EMI
8	On	Full duplex	CRC error	OK	EMI
9	Off	Half duplex	None	OK	
10	Off	Half duplex	Collisions	OK	
11	Off	Half duplex	Late collisions	Duplex problem detected	Duplex problem, EMI, network extension
12	Off	Half duplex	CRC error	OK	EMI
13	Off	Full duplex	None	OK	
14	Off	Full duplex	Collisions	OK	EMI
15	Off	Full duplex	Late collisions	OK	EMI
16	Off	Full duplex	CRC error	Duplex problem detected	Duplex problem, EMI

Table 27: Evaluation of non-matching of the duplex mode

Activating the detection

☐ Select the `Switching:Global` dialog.

☐ Select “Enable duplex mismatch detection”. The Magnum 12KX then checks whether the duplex mode of a port might not match that of the remote port.
If the Magnum 12KX detects a potential mismatch, it creates an entry in the event log and sends an alarm (trap).

`enable`	**Switch to the Privileged EXEC mode.**
`configure`	**Switch to the Configuration mode.**
`bridge duplex-mismatch-detect operation enable`	**Activates the detection and reporting of non-matching duplex modes.**
`bridge duplex-mismatch-detect operation disable`	**Deactivates the detection and reporting of non-matching duplex modes.**

FIGURE 133 – Activating detection and reporting of non-matching duplex modes using CLI

Displaying the SFP Status

The SFP status display allows user to look at the current SFP module connections and their properties. The properties include:

- module type
- support provided in media module
- Temperature in ºC
- Tx Power in mW
- Receive power in mW

☐ Select the `Diagnostics:Ports:SFP Modules` dialog.

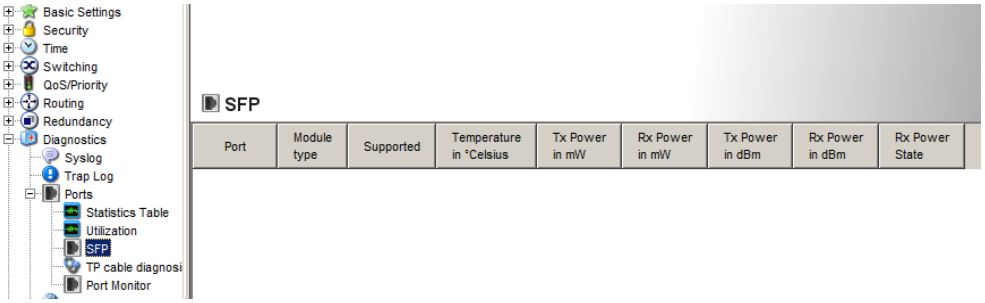


FIGURE 134 – Device SFP Modules

TP Cable Diagnosis

The TP cable diagnosis allows user to check the connected cables for short-circuits or interruptions.

Note: While the check is running, the data traffic at this port is suspended.

The check takes a few seconds. After the check, the "Result" row contains the result of the cable diagnosis. If the result of the check shows a cable problem, then the "Distance" row contains the cable problem location's distance from the port.

Result	Meaning
normal	The cable is okay.
open	The cable is interrupted.
short circuit	There is a short-circuit in the cable.
unknown	No cable check was performed yet, or it is currently running

Table 28: Meaning of the TP cable diagnostic results

Prerequisites for correct TP cable diagnosis:

- 1000BASE-T port, connected to a 1000BASE-T port via 8-core cable or
- 10BASE-T/100BASE-TX port, connected to a 10BASE-T/100BASE-TX port.

☐ Select the `Diagnostics:Ports:TP cable diagnosis` dialog.

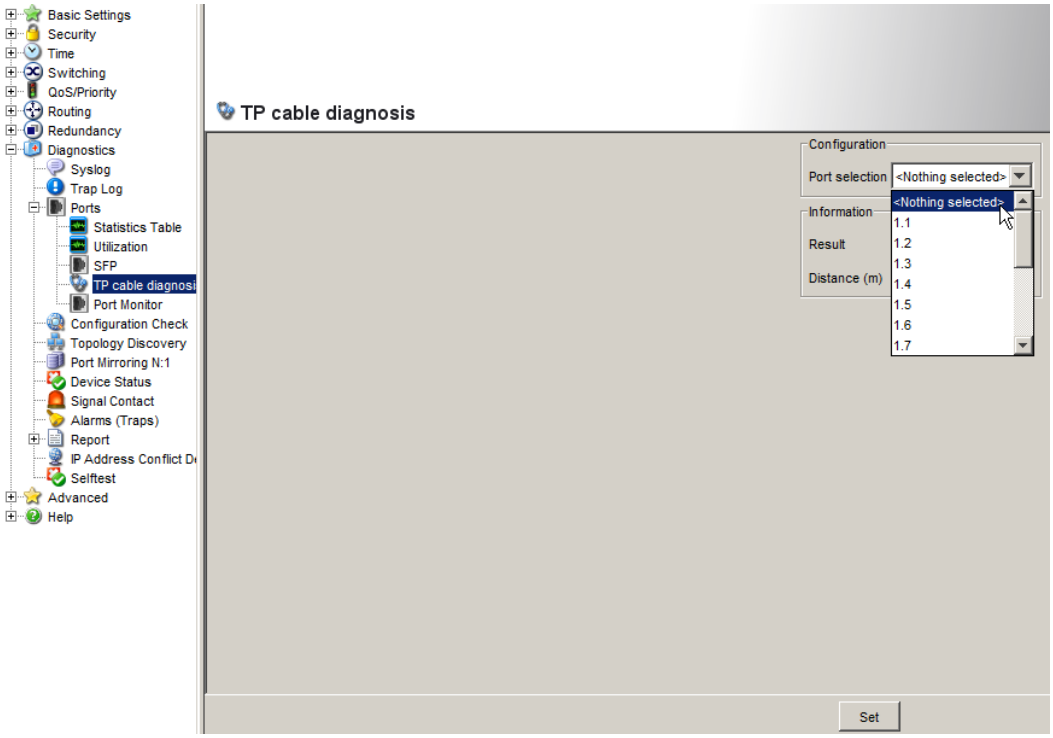


FIGURE 135 – Device TP Diagnostics

☐ Select a TP port at which needs to be checked.

☐ Click on “Set” to start the check.

Topology Discovery

IEEE 802.1AB describes the Link Layer Discovery Protocol (LLDP). LLDP enables the user to have automatic topology recognition for his LAN.

A device with active LLDP

- sends its own connection and management information to neighboring devices of the shared LAN. This can be evaluated there once these devices have also activated LLDP.
- receives connection and management information from neighboring devices of the shared LAN, once these devices have also activated LLDP.
- sets up a management information schema and object definition for saving information of neighboring devices with active LLDP.

A central element of the connection information is the exact, unique ID of a connection point: MSAP (MAC Service Access Point). This is made up of a device ID unique within the network and a port ID unique for this device.
Content of the connection and management information:

- Chassis ID (its MAC address)
- Port ID (its port MAC address)
- Description of the port

- System Name
- System description
- Supported system capabilities
- Currently activated system capabilities
- Interface ID of the management address
- Port VLAN ID of the port
- Status of the autonegotiation at the port
- Medium, half and full duplex settings and speed setting of the port
- Information about whether a redundancy protocol is switched on at the port, and which one (for example, RSTP, HIPER-Ring, Fast-HIPER-Ring, MRP, Ring Coupling).
- Information about the VLANs which are set up in the switch (VLAN ID and VLAN name, regardless of whether the port is a VLAN member).

A network management station can call up this information from a device with LLDP activated. This information enables the network management station to map the topology of the network.

To exchange information, LLDP uses an IEEE MAC address which devices do not usually send. For this reason, devices without LLDP support discard LLDP packets. Thus a non-LLDP-capable device between 2 LLDP-capable devices prevents LLDP information exchange between these two devices. To get around this, Belden (GarrettCom and Hirschmann) devices send and receive additional LLDP packets with the GarrettCom and Hirschmann Multicast MAC address 01:80:63:2F:FF:0B. GarrettCom and Hirschmann devices with the LLDP function are thus also able to exchange LLDP information with each other via devices that are not LLDP-capable.

The Management Information Base (MIB) of an LLDP-capable GarrettCom and Hirschmann device holds the LLDP information in the LLDP MIB and in the private LLDP.

Displaying the Topology Discovery Results

☐ Select the `Diagnostics:Topology Discovery` dialog.

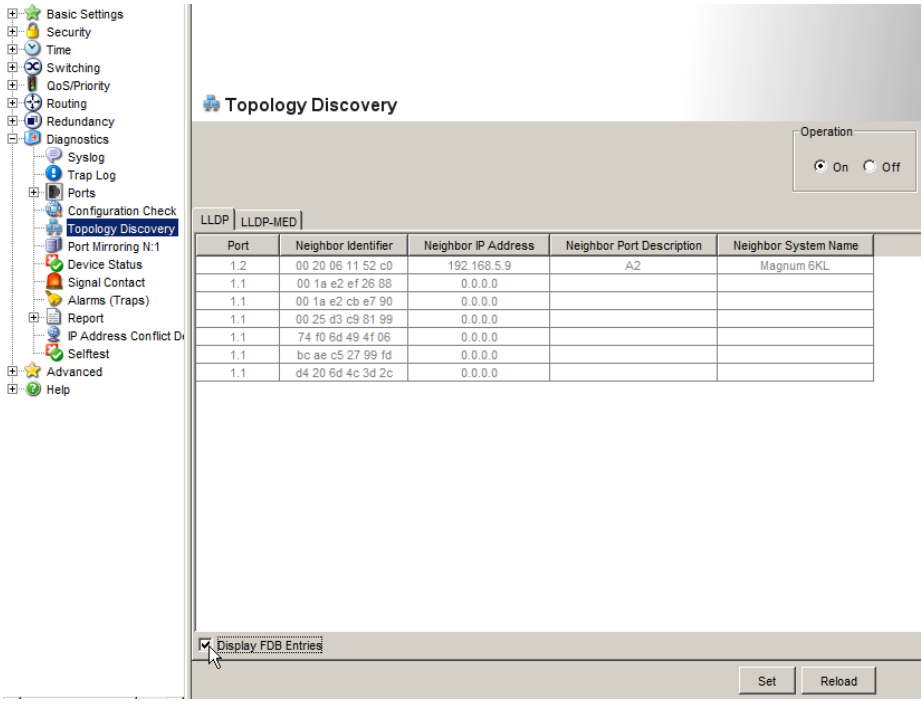


FIGURE 136 – Topology Discovery

This dialog allows user to switch on/off the topology discovery function (LLDP). The topology table shows the collected information for neighboring devices. This information enables the network management station to map the structure of the network.

The option "Display FDB Entries" allows user to reduce the number of table entries. In this case, the topology table hides entries from devices without active LLDP support.

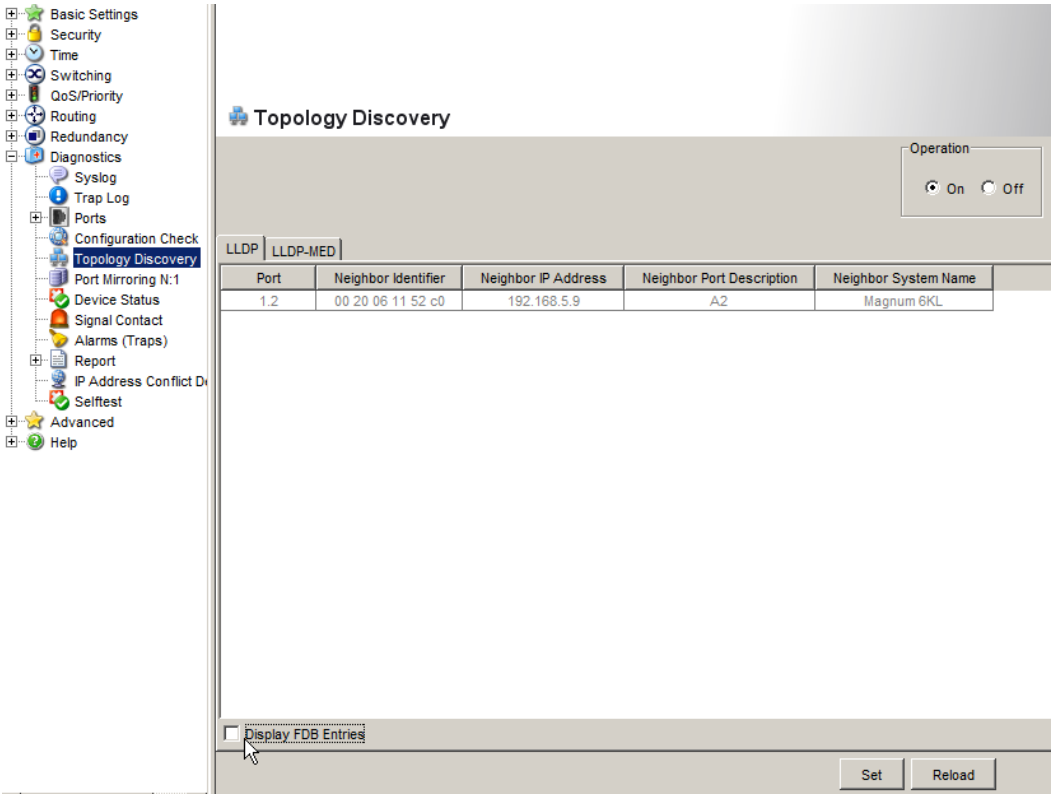


FIGURE 137 – Reduced entries with the “Display FDB Entries” unchecked.

If several devices are connected to one port, for example via a hub, the table will contain one line for each connected device.

If

- devices with active topology discovery function and
- devices without active topology discovery function

are connected to a port, the topology table hides the devices without active topology discovery.

If

- only devices without active topology discovery are connected to a port, the table will contain one line for this port to represent all devices. This line contains the number of connected devices.
  MAC addresses of devices that the topology table hides for the sake of clarity, are located in the address table (FDB).

Detecting IP Address Conflicts

By definition, each IP address may only be assigned once within a subnetwork. Should two or more devices erroneously share the same IP address within one subnetwork, this will inevitably lead to communication disruptions with devices that have this IP address. In his Internet draft, Stuart Cheshire describes a mechanism that industrial Ethernet devices can use to detect and eliminate address conflicts (Address Conflict Detection, ACD).

Mode	Meaning
enable	Enables active and passive detection.
disable	Disables the function
activeDetectionOnly	Enables active detection only. After connecting to a network or after an IP address has been configured, the Magnum 12KX immediately checks whether its IP address already exists within the network. If the IP address already exists, the Magnum 12KX will return to the previous configuration, if possible, and make another attempt after 15 seconds. This prevents the Magnum 12KX from connecting to the network with a duplicate IP address.
passiveOnly	Enables passive detection only. The Magnum 12KX listens passively on the network to determine whether its IP address already exists. If it detects a duplicate IP address, it will initially defend its address by employing the ACD mechanism and sending out gratuitous ARPs. If the remote device does not disconnect from the network, the management interface of the local device will then disconnect from the network. Every 15 seconds, it will poll the network to determine if there is still an address conflict. If there isn't, it will connect back to the network.

Table 29: Possible address conflict operation modes

Configuring ACD

- ☐ Select the `Diagnostics:IP Address Conflict Detection` dialog.
- ☐ With "Status" enable/disable the IP address conflict detection or select the operating mode (See table above).

Displaying ACD

- ☐ Select the `Diagnostics:IP Address Conflict Detection` dialog.

- In the table the Magnum 12KX logs IP address conflicts with its IP address.
  For each conflict the Magnum 12KX logs:
  - the time
  - the conflicting IP address
  - the MAC address of the device with which the IP address conflicted.

  For each IP address, the Magnum 12KX logs a line with the last conflict that occurred.

☐ This table can be deleted by restarting the Magnum 12KX.

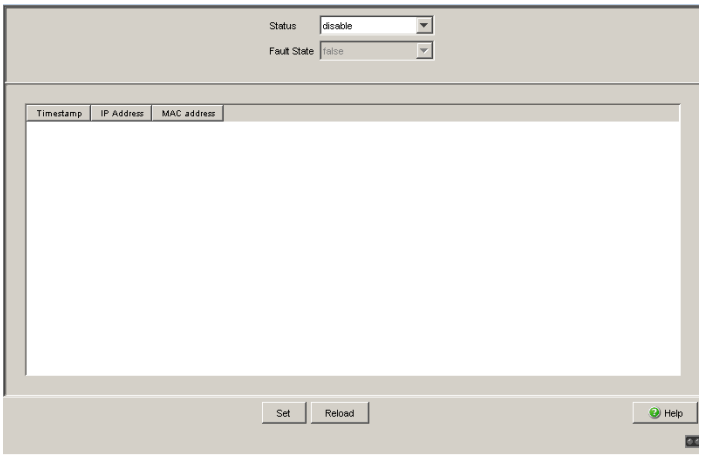


FIGURE 138 – IP Address Conflict Detection dialog

Detecting Loops

Loops in the network, even temporary loops, can cause connection interruptions or data losses. The automatic detection and reporting of this situation allows the user to detect it faster and diagnose it more easily.

An incorrect configuration can cause a loop, for example, if Spanning Tree is deactivated.

The Magnum 12KX allows the user to detect the effects typically caused by loops and report this situation automatically to the network management station. Users have the option here to specify the magnitude of the loop effects that triggers the Magnum 12KX to send a report.

A typical effect of a loop is that frames from multiple different MAC source addresses can be received at different ports of the Magnum 12KX within a short time. The Magnum 12KX evaluates how many of the same MAC source addresses it has learned at different ports within a time period.

Note: This procedure detects loops when the same MAC address is received at different ports. However, loops can also have other effects.
And it is also the case that the same MAC address being received at different ports can have other causes.

☐ Select the `Switching:Global` dialog.

☐ Select “Activate address relearns detection”. Enter the desired threshold value in the “Address relearn threshold” field.

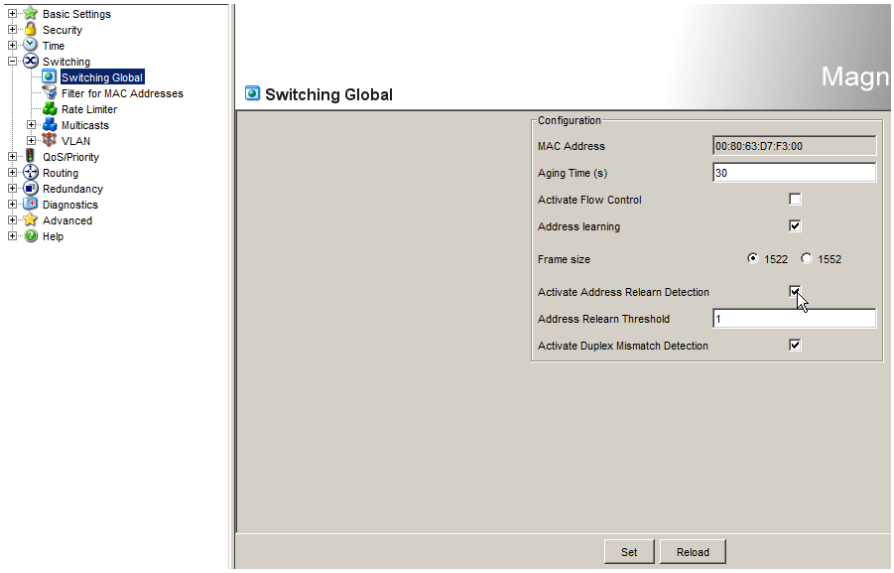


FIGURE 139 – Activating Address Learning

If the address relearns detection is enabled, the Magnum 12KX checks whether it has repeatedly learned the same MAC source addresses at different ports. This process very probably indicates a loop situation.
If the Magnum 12KX detects that the threshold value set for the MAC addresses has been exceeded at its ports during the evaluation period (a few seconds), the Magnum 12KX creates an entry in the log file and sends an alarm (trap). The preset threshold value is 1.

Reports

The following reports and buttons are available for the diagnostics:

- Log file.
  The log file is an HTML file in which the Magnum 12KX writes all the important device-internal events.
- System information.
  The system information is an HTML file containing all system-relevant data.
- Download Switch-Dump.
  This button allows user to download system information as files in a ZIP archive.

In service situations, these reports provide the technician with the necessary information.

The following button is available as an alternative for operating the Web-based interface:

- Download JAR file.
  This button allows user to download the applet of the Web-based interface as a JAR file. Afterwards there is the option to start the applet outside a browser.
  This enables user to administer the Magnum 12KX even when the Web server has been deactivated for security reasons.

☐ Select the `Diagnostics:Report` dialog.

☐ Click “Log File” to open the HTML file in a new browser window.

☐ Click “System Information” to open the HTML file in a new browser window.

☐ Click “Download Switch-Dump”.

☐ Select the directory in which to save the switch dump.

☐ Click “Save”.

The Magnum 12KX creates the file name of the switch dumps automatically in the format <IP address>_<system name>.zip

☐ Click “Download JAR-File”.

☐ Select the directory in which to save the applet.

☐ Click “Save”.

The Magnum 12KX creates the file name of the applet automatically in the format <device type><software variant><software version)>_<software revision of applet>.jar

Chapter 13

Port Mirroring

The port mirroring function enables the user to review the data traffic at up to 8 ports of the Magnum 12KX for diagnostic purposes. The Magnum 12KX additionally forwards (mirrors) the data for these ports to another port. This process is also called port mirroring.
The ports to be reviewed are known as source ports. The port to which the data to be reviewed is copied is called the destination port. Only physical ports can be used as source or destination ports.

In port mirroring, the Magnum 12KX copies valid incoming **and** outgoing data packets of the source port to the destination port. The Magnum 12KX does not affect the data traffic at the source ports during port mirroring.
A management tool connected at the destination port, e.g. an RMON probe, can thus monitor the data traffic of the source ports in the sending and receiving directions.

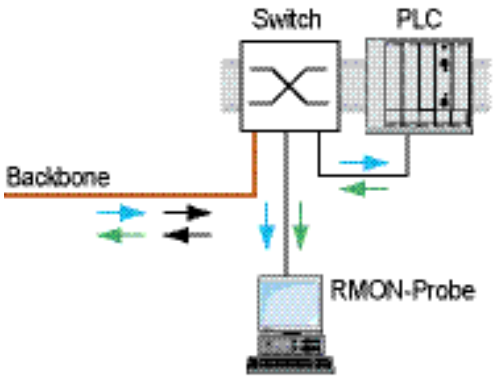


FIGURE 140 – Port mirroring

☐ Select the `Diagnostics:Port Mirroring` dialog.

This dialog allows user to configure and activate the port mirroring function of the Magnum 12KX.

- ☐ Select the source ports whose data traffic that need review from the list of physical ports by check marking the relevant boxes.
  A maximum of 8 source ports can be selected. Ports that cannot be selected are displayed as inactive by the Magnum 12KX, e.g. the port currently being used as the destination port, or there are already 8 ports selected. Default setting: no source ports.
- ☐ Select the destination port to which the management tool is connected from the list element in the “Destination Port” frame.
  The Magnum 12KX does not display ports that cannot be selected in the list, e.g. the ports currently being used as source ports. Default setting: port 0.0 (no destination port).
- ☐ Select “On” in the “Function” frame to switch on the function. Default setting: “Off”.

The “Reset configuration” button in the dialog allows user to reset all the port mirroring settings of the Magnum 12KX to the state by default.

Note: When port mirroring is active, the specified destination port is used solely for reviewing, and does not participate in the normal data traffic.

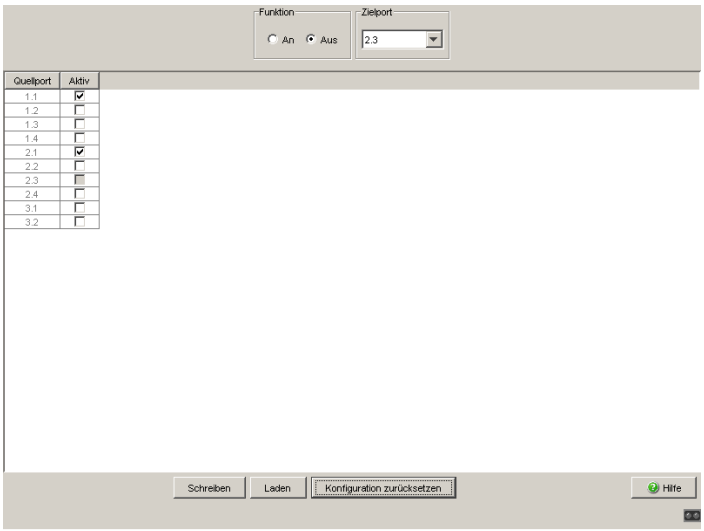


FIGURE 141 – Port Mirroring dialog

Chapter 14

Syslog

The Magnum 12KX enables user to send messages about important device-internal events to up to 8 Syslog servers. Additionally, user can also include SNMP requests to the Magnum 12KX as events in the syslog.

Note: The actual events that the Magnum 12KX has logged can be found in the “Event Log” dialog and in the log file a HTML page with the title “Event Log”.

☐ Select the `Diagnostics:Syslog` dialog.

☐ Activate the syslog function in the “Operation” frame.

☐ Click on “Create”.
☐ In the “IP Address” column, enter the IP address of the syslog server to which the log entries should be sent.
☐ In the “Port” column, enter the UDP port of the syslog server at which the syslog receives log entries. The default setting is 514.
☐ In the “Minimum level to report” column, enter the minimum level of seriousness an event must attain for the Magnum 12KX to send a log entry to this syslog server.
☐ In the “Active” column, select the syslog servers that the Magnum 12KX takes into account when it is sending logs.

“SNMP Logging” frame:
☐ Activate “Log SNMP Get Request” if reading SNMP requests need to be sent to the Magnum 12KX as events to the syslog server.
☐ Select the level to report at which the device creates the events from reading SNMP requests.
☐ Activate “Log SNMP Set Request” if writing SNMP requests need to be sent to the Magnum 12KX as events to the syslog server.
☐ Select the level to report at which the Magnum 12KX creates the events from writing SNMP requests.

Note: For more details on setting the SNMP logging, see the “Syslog” chapter in the “Web-based Interface” reference manual.

`enable`	**Switch to the Privileged EXEC mode.**
`configure`	**Switch to the Configuration mode.**
`logging host 10.0.1.159 514 3`	**Select the recipient of the log messages and its port 514. The “3” indicates the seriousness of the message sent by the**

device. “3” means “error”.

```
logging syslog                Enable the Syslog function.
exit                            Switch to the privileged EXEC mode.
show logging hosts            Display the syslog host settings.
Index     IP Address        Severity   Port     Status
-----  -----------------  ----------  ----  -------------
1      10.0.1.159          error       514   Active

enable                        Switch to the Privileged EXEC mode.
configure                     Switch to the Configuration mode.
logging snmp-requests         Create log events from reading SNMP requests.
get operation enable
logging snmp-requests          The “5” indicates the seriousness of the message that the
get  severity 5               Magnum 12KX allocates to messages from reading SNMP
                              requests. “5” means “note”.
logging snmp-requests         Create log events from writing SNMP requests.
set operation enable
logging snmp-requests          The “5” indicates the seriousness of the message that the
set severity 5                Magnum 12KX allocates to messages from writing SNMP
                              requests. “5” means “note”.
exit                          Exit the privileged EXEC mode.
show logging                  Display the SNMP logging settings.
snmp-requests
Log SNMP SET requests                    : enabled
Log SNMP SET severity                    : notice
Log SNMP GET requests                    : enabled
Log SNMP GET severity                    : notice
```

FIGURE 142 – Configuring Syslog using CLI

Event Log

The Magnum 12KX allows users to call up a log of the system events. The table of the “Event Log” dialog lists the logged events with a time stamp.

- ☐ Click on “Load” to update the content of the event log.
- ☐ Click on “Delete” to delete the content of the event log.

Note: Users have the option to also send the logged events to one or more syslog servers.

Chapter 15

Access via SSH

To be able to access the Magnum 12KX via SSH, users will need:
- a key
- to install the key on the Magnum 12KX
- to enable access via SSH on the Magnum 12KX
- and a program for executing the SSH protocol on the computer.

Generating a SSH Host Key

The program PuTTYgen allows users to generate a key. This program can be downloaded from the web (e.g. from sourceforge.net or other such mirror locations).

☐ Start the program by double-clicking on it.
☐ In the main window of the program, within the “Parameter” frame, select the type “SSH-1 (RSA)”.
☐ In the “Actions” frame, click “Generate”. Move the mouse so that PuTTYgen can generate the key using random numbers.
☐ Under “Key passphrase” and “Confirm passphrase” do not enter a password for this key.
☐ In the “Actions” frame, click “Save private key”.
Enter the file name and the storage location for the key file.
☐ Answer the question about not wanting to use a passphrase with “Yes”.
☐ Make a note of the fingerprint of the key in order to check the connection setup.
☐ Also store the key separately from the Magnum 12KX so that if the device is replaced it can be transferred to the replacement device.

FIGURE 143 – PuTTY key generator

The OpenSSH Suite offers experienced network administrators a further option for generating the key. To generate the key, enter the following command:

```
ssh-keygen(.exe) -q -t rsa1 -f rsa1.key -C '' -N ''
```

Uploading the SSH Host Key

The Command Line Interface enables the upload of the SSH key to the Magnum 12KX.

☐ Store the key file on the tftp server.

`enable`	**Switch to the Privileged EXEC mode.**
`no ip ssh`	**Deactivate the SSH function on the Magnum 12KX before transferring the key to the device.**
`copy tftp://10.0.10.1/-device/rsa1.key nvram:sshkey-rsa1`	**The Magnum 12KX loads the key file to its non-volatile memory.** **`10.0.10.1` represents the IP address of the tftp server.** **`device` represents the directory on the tftp server.** **`rsa1.key` represents the file name of the key.**
`ip ssh`	**Reactivate the SSH function after transferring the key to the device.**

FIGURE 144 – Uploading the SSH Key using CLI

Access via SSH

The program PuTTY enables the access of the Magnum 12KX via SSH. This program can be downloaded from the web (e.g. sourceforge.net or other such mirror sites.)

☐ Start the program by double-clicking on it.
☐ Enter the IP address of the Magnum 12KX.
☐ Select “SSH”.
☐ Click “Open” to set up the connection to the Magnum 12KX.
Depending on the device and the time at which SSH was configured, it can take up to a minute to set up the connection.

Shortly before the connection is set up, PuTTY displays a security alert message and provides the option of checking the fingerprint of the key.

FIGURE 145 – Security alert prompt for the SSH key

☐ Check the fingerprint to protect from unwelcome guests. The fingerprint is located in the “Key” frame of the PuTTY key generator.
☐ If the fingerprint matches the key, click “Yes”.

PuTTY will display another security alert message for the warning threshold set.

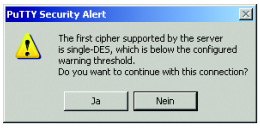


FIGURE 146 – Security alert prompt for the warning threshold set

☐ Click “Yes” for this security alert message.

To suppress this message for future connection set-ups, select “SSH” in the “Category” frame before a connection is set up in PuTTY. In the “Encryption options” frame, select “DES” and then click “Up” until “DES” is above the line “---warn below here --”. In the “Category” frame, go back to Session and set up a connection in the usual way.

The OpenSSH Suite offers experienced network administrators a further option to access the Magnum 12KX via SSH. To set up the connection, enter the following command:

```
ssh admin@10.0.112.53 -cdes
```

`admin` represents the user name.
`10.0.112.53` is the IP address of the Magnum 12KX.
`-cdes` specifies the encryption for SSHv1

Chapter 16

Routing Basics

A router is a node for exchanging data on the layer 3 of the ISO/OSI layer model.
This ISO/OSI reference model had the following goals:

To define a standard for information exchange between open systems;
To provide a common basis for developing additional standards for open systems;
To provide international teams of experts with functional framework as the basis for independent development of every layer of the model;
To include in the model developing or already existing protocols for communications between heterogeneous systems;
To leave sufficient room and flexibility for the inclusion of future developments.

The reference model consists of 7 layers, ranging from the application layer to the physical layer.

7	Application	Access to communication services from an application program
6	Presentation	Definition of the syntax for data communication
5	Session	Set up and breakdown of connections by synchronization and organization of the dialog
4	Transport	Specification of the terminal connection, with the necessary transport quality
3	Network	Transparent data exchange between two transport entities
2	Data-Link	Access to physical media and detection of transmission errors
1	Physical	Transmission of bit strings via physical media

Table 30: OSI Reference Model

What does the data exchange on the layer 3 mean in comparison with the data exchange on the layer 2?

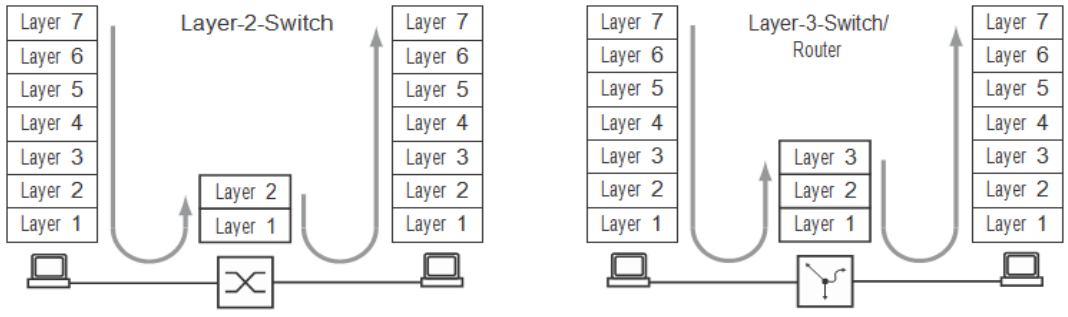


FIGURE 147 – Data Transport by a Switch and a Router in the OSI Reference Model's Layers

On the layer 2, the MAC address signifies the destination of a data packet. The MAC address is an address tied to the hardware of a device. The layer 2 expects the receiver in the connected network. The data exchange to another network is the task of layer 3. Layer 2 data traffic is spread over the entire network. Every subscriber filters the data relevant for him from the data stream. Layer 2 switches are capable of steering the data traffic that is intended for a specific MAC address. It thus relieves some of the load on the network. Broadcast and multicast data packets are forwarded by the layer 2 switches at all ports.

IP is a protocol on the layer 3. IP provides the IP address for addressing data packets. The IP address is assigned by the network administrator. By systematically assigning IP addresses, he can thus structure his network breaking it down into subnets . The bigger a network gets, the greater the data volume. Because the available bandwidth has physical limitations, the size of a network is also limited. Dividing large networks into subnets limits the data volume on these subnets. Routers divide the subnets from each other and only transmit the data that is intended for another subnet.

FIGURE 148 – MAC Data Transmission: Unicast Data Packet (left) and Broadcast Data Packet (right)

This illustration clearly shows that broadcast data packets can generate a considerable load on larger networks. Networks can be made easier to understand by forming subnets, which can be connected with each other using routers and, strange as it sounds, also separate securely from each other.

A Switch uses the MAC destination address to transmit, and thus uses layer 2.

A router uses the IP destination address to transmit, and thus uses layer 3. The subscribers associate the MAC and IP addresses using the Address Resolution Protocol (ARP)

ARP

The Address Resolution Protocol (ARP) determines the MAC address that belongs to an IP address. What is the benefit of this?

Let's suppose that the user wants to configure the Switch using the Web-based interface. Enter the IP address of the Switch in the address line of the browser. But which MAC address will the PC now use to display the information in the Switch in the browser window?

If the IP address of the Switch is in the same subnet as the PC, then the PC sends what is known as an ARP request. This is a MAC broadcast data packet that requests the owner of the IP address to send back his MAC address. The Switch replies with a unicast data packet containing his MAC address. This unicast data packet is called an ARP reply.

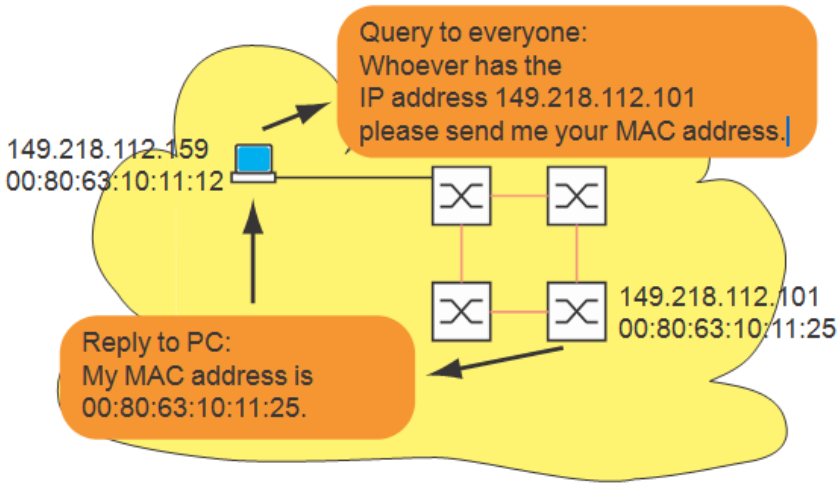


FIGURE 149 – ARP request and reply

If the IP address of the Switch is in a different subnet, then the PC asks for the MAC address of the gateway entered in the PC. The gateway/router replies with its MAC address. Now the PC packs the IP data packet with the IP address of the switch, the final destination, into a MAC frame with the MAC destination address of the gateway/router and sends the data. The router receives the data and releases the IP data packet from the MAC frame, so that it can then forward it in accordance with its transmission rules.

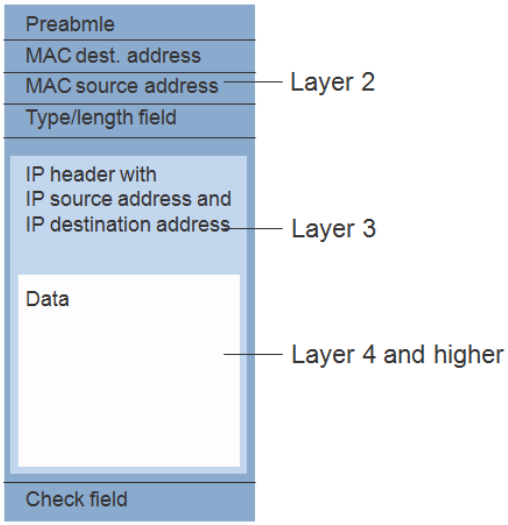


FIGURE 150 – Structure of a data packet from the ISO/OSI layer model perspective

All terminal devices still working with IPs of the first generation, for example, are not yet familiar with the term 'subnet'. They also send an ARP request when they are looking for the MAC address for an IP address in a different subnet. They neither have a network mask with which they could recognize that the subnet is a different one, nor do they have a gateway entry. In the example below, the left PC is looking for the MAC address of the right PC, which is in a different subnet. In this example, it would normally not get a reply.

Because the router knows the route to the right PC, the proxy ARP function replies to this router interface on behalf of the right PC with its own MAC address. Thus the left PC can address its data to the MAC address of the router, which then forwards the data to the right PC.

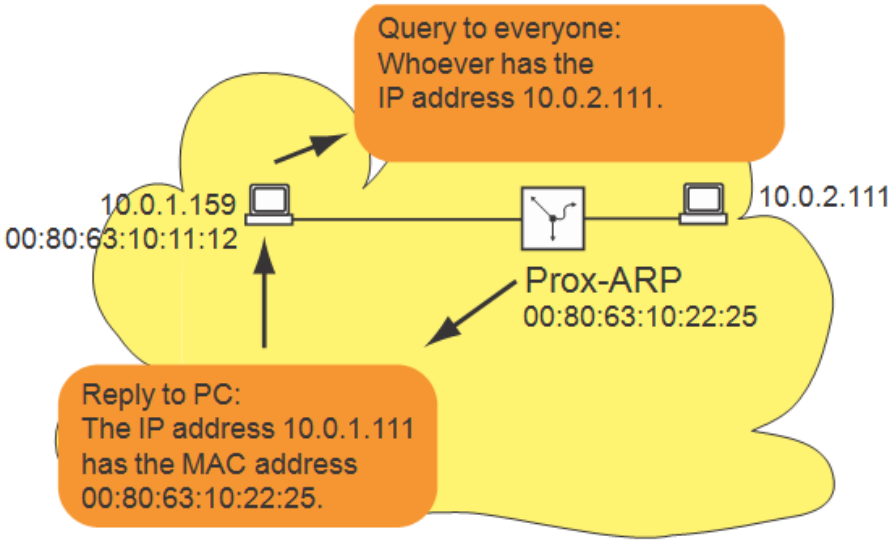


FIGURE 151 – ARP proxy function

The proxy ARP function is available on the router interfaces on which you switch on the proxy ARP.

CIDR

The original class allocation of the IP addresses only planned for three address classes to be used by the users (see “Basics of IP Parameters” in the basic configuration of the user manual).

Since 1992, five classes of IP address have been defined in the RFC-1340.

Class	Network part	Host part	Address range
A	1 byte	3 bytes	1.0.0.0 to 126.255.255.255
B	2 bytes	2 bytes	128.0.0.0 to 191.255.255.255
C	3 bytes	1 byte	192.0.0.0 to 223.255.255.255
D			224.0.0.0 to 239.255.255.255
E			240.0.0.0 to 255.255.255.255

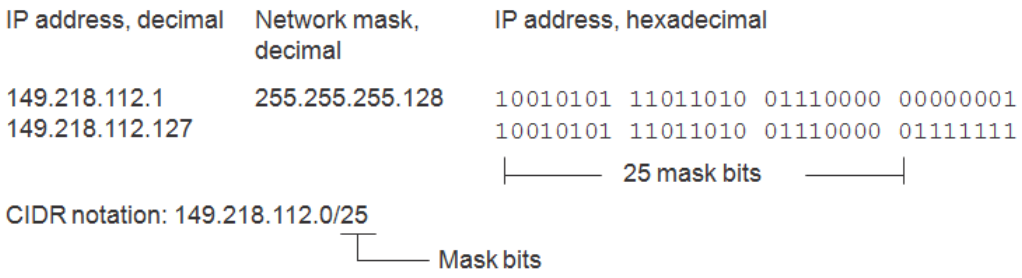
Table 31: IP address classes

Class C with a maximum of 254 addresses was too small, and class B with a maximum of 65534 addresses was too large for most users, as they would never require so many addresses. This resulted in ineffective usage of the class B addresses available.

Class D contains reserved multicast addresses. Class E is reserved for experimental purposes. A gate-

way not participating in these experiments ignores datagrams with this destination address.The Classless Inter-Domain Routing (CIDR) provides a solution to these problems. The CIDR overcomes these class boundaries and supports
classless address ranges.

With CIDR, enter the number of bits that designate the IP address range. Represent the IP address range in binary form and count the mask bits that designate the network mask. The network mask indicates the number of bits that are identical for all IP addresses, the network part, in a given address range. Example:



The combination of a number of class C address ranges is known as “supernetting”. This enables the user to subdivide class B address ranges to a very fine degree.

Using mask bits simplifies the routing table. The router determines in that direction in which most of the mask bits match (longest prefix match).

Net-directed Broadcasts

A net-directed broadcast is an IP data packet that a device sends to a net‘s broadcast address[1] to address all receivers of that net. In a transfer network, a net-directed broadcast is sent as a MAC unicast frame. If the router locally responsible for that network supports net-directed broadcasts, it sends these data packets as MAC broadcast frame to its local network. If the router interface is VLAN based, the router sends the frame to all ports that are members of the router interface VLAN.

This way, net-directed broadcasts can relieve the transfer network from multiple IP unicasts which would be necessary as alternative for a net- directed broadcast.

If the router does not support net-directed broadcasts, or if this function is deactivated for a router interface, the router discards the received IP data packets which have been sent to the router interface‘s network broadcast address. In case of multinetting, this applies also to the router interface‘s secondary IP addresses.

Multinetting

[1] The net broadcast address is the topmost IP address of an IP network for which a router interface is responsible. The device determines the broadcast address from an interface IP address and the corresponding network mask. If a router interface has e.g. the IP address 192.168.1.1 and the network mask 255.255.255.0, it is responsible for the network 192.168.1.0/24. The net broadcast address is in this case 192.168.1.255

Multinetting allows the user to connect a number of subnets to one router port. Multinetting provides a solution when existing subnets need to be connected to a router within a physical medium. In this case multinetting can be used to assign a number of IP addresses for the different subnets to the routing port to which the physical medium is being connected.

For a long-term solution, other network design strategies provide more advantages with regard to problem solving and bandwidth management.

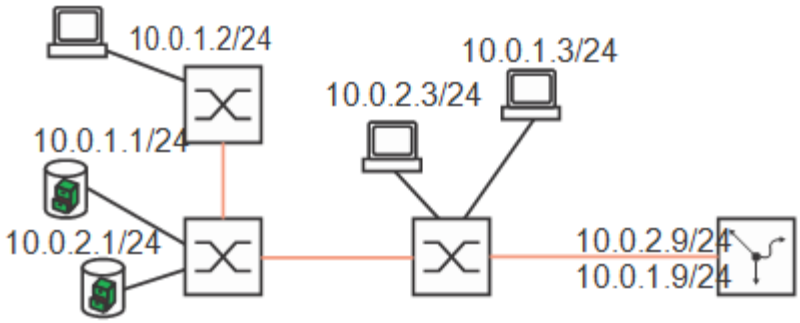


FIGURE 152 – Example of multinetting

Chapter 17

Static Routing

Static routes are user-defined routes which the Switch uses to transmit data from one subnet to another. The user specifies to which router (next hop) the Switch forwards data for a particular subnet. Static routes are kept in a table which is permanently stored in the Switch.

Compared to dynamic routing, the advantage of this transparent route selection is offset by the increased workload involved in configuring the static routes. Static routing is therefore suited to very small networks or to selected areas of larger networks. Static routing makes the routes transparent for the administrator and can be easily configured in small networks. If, for example, a line interruption causes the topology to change, the dynamic routing can react automatically to this, in contrast to the static routing. If static and dynamic routing are combined, the static routes can be configured in such a way that they have a higher priority than a route selected by a dynamic routing procedure.

The first step in configuring the router is to globally switch on the router function and configure the router interfaces. The Switch allows the user to define port-based and VLAN-based router interfaces.

Example: Connecting two production cells

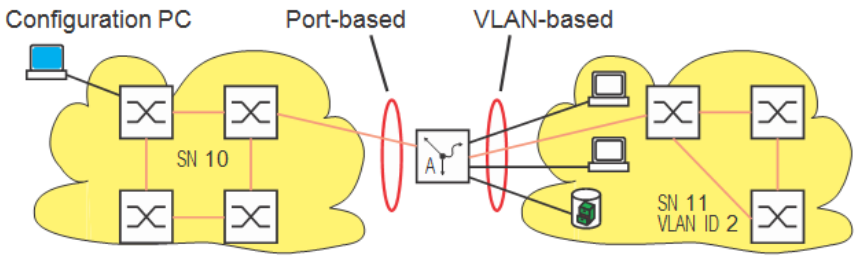


FIGURE 153 – Static routes

Port-based Router Interface

A characteristic of the port-based router interface is that a subnet is connected to a port.

Special features of port-based router interfaces:

- If there is no active connection, then the entry from the routing table is omitted, because the router transmits exclusively to those ports for which the data transfer is likely to be successful.
- The entry in the interface configuration table remains.
- A port-based router interface does not recognize VLANs, which means that the router rejects tagged frames which it receives at a port-based router interface.
- A port-based router interface rejects all the non-routable packets.

Below is an example of the simplest case of a routing application with port-based router interfaces.

Configuration of the Router Interfaces

FIGURE 154 – Simplest case of a router

`enable`	**Switch to the Privileged EXEC mode.**
`configure`	**Switch to the Configuration mode.**
`interface 1/5`	**Select the interface for which the IP address needs to be entered**
`ip address 10.0.1.1 255.255.255.0`	**Assign the IP parameters to the port**
`routing`	**Enable routing on the port**
`exit`	**Switch to configuration mode**
`interface 1/6`	**Select the second port for the IP address**
`ip address 10.0.2.1 255.255.255.0`	**Set the IP address**
`routing`	**Enable routing on the interface**
`ip netdirbcast`	**Switch on the transmission of the net-directed broadcast**
`exit`	**Exit Configuration mode**
`exit`	**Exit EXEC mode**
`show ip interface brief`	**Verify the entries**

```
                                                Netdir    Multi
Interface IP Address      IP Mask               Bcast     CastFwd
--------- --------------- --------------- -------- --------
1/5       10.0.1.1        255.255.255.0   Disable  Disable
1/6       10.0.2.1        255.255.255.0   Enable   Disable
```

`show ip interface 1/5` Verify the settings of port 1/5

```
Primary IP Address.............................. 10.0.1.1/255.255.255.0
Routing Mode.................................... Enable
Administrative Mode............................. Enable
Forward Net Directed Broadcasts................. Disable
Proxy ARP....................................... Disable
Active State.................................... Active
Link Speed Data Rate............................ 100 Full
MAC Address..................................... 00:80:63:D7:F3:0C
Encapsulation Type.............................. Ethernet
IP MTU.......................................... 1500
```

```
show ip route                    Verify the routing table
Total Number of Routes..................... 2

   Network          Subnet                    Next Hop    Next Hop
   Address           Mask         Protocol      Intf     IP Address
--------------- --------------- ------------  ------  ---------------
10.0.1.0        255.255.255.0    Local         1/5      10.0.1.1
10.0.2.0        255.255.255.0    Local         1/6      10.0.2.1

show ip route bestroutes     Check the routes the 12KX switch uses

Total Number of Routes..................... 2

   Network          Subnet                    Next Hop    Next Hop
   Address           Mask         Protocol      Intf     IP Address
--------------- --------------- ------------  ------  ---------------
10.0.1.0        255.255.255.0    Local         1/5      10.0.1.1
10.0.2.0        255.255.255.0    Local         1/6      10.0.2.1
```

FIGURE 155 – Configuring Router Interfaces using CLI

☐ The interface IP address can be set via the Routing: Interfaces: Configuration menu as shown below.

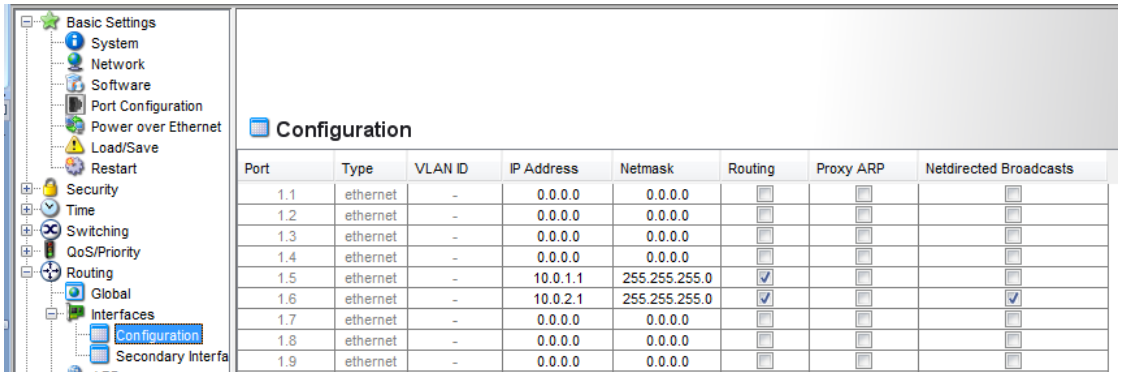


FIGURE 156 – Static route entries for the ports

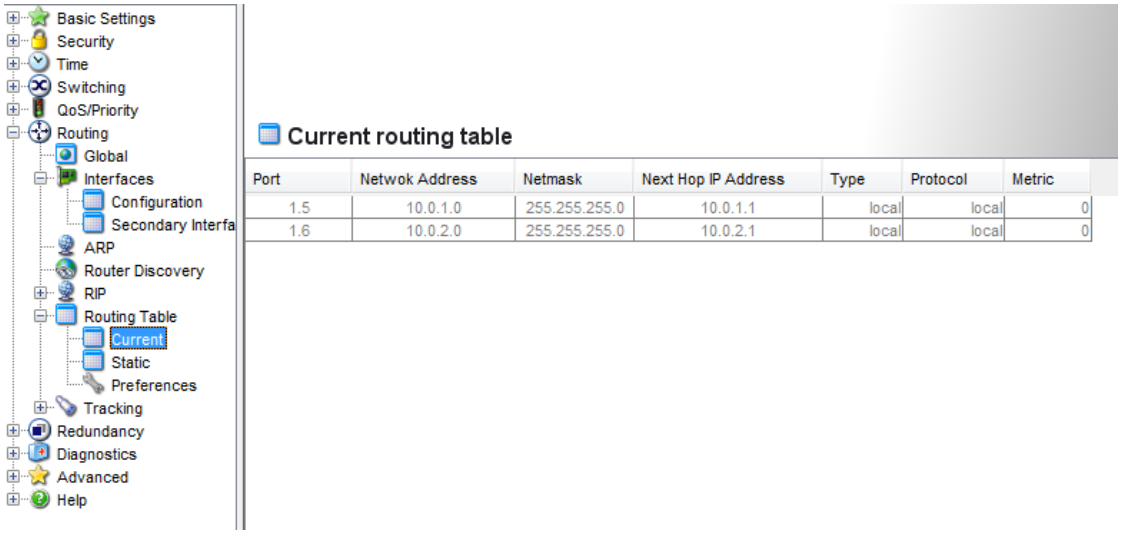


FIGURE 157 – Display the routing information

Note: To be able to see these entries in the routing table, an active connection to the ports is needed.

VLAN-based Router-Interface

A characteristic of the VLAN-based router interface is that a number of devices in a VLAN are connected to different ports. The devices within a subnet belong to one VLAN.

Within a VLAN, the Switch exchanges data packets on layer 2. Terminal devices address data packets with a destination address in another subnet to the router as a gateway. The router then exchanges the data packets layer 3.

Below is an example of the simplest case of a routing application with VLAN-based router interfaces. For the VLAN 2, the router combines ports 3.1 and 3.2 into the VLAN router interface 9.1. A VLAN router interface remains in the routing table until at least one port of the VLAN has a connection.

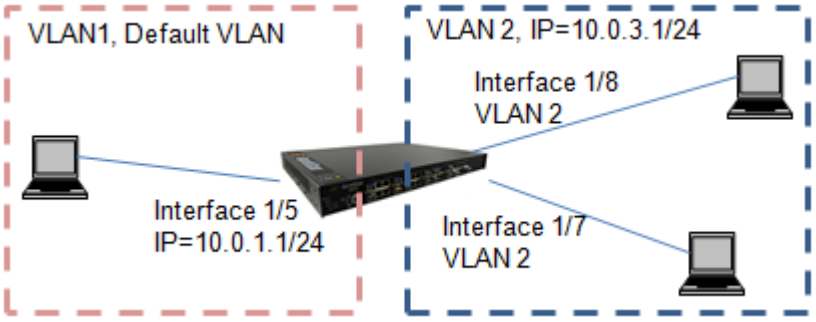


FIGURE 158 – VLAN-based router interface

Configure a VLAN route interface:

```
enable                          Switch to the Privileged EXEC mode.
vlan database                   Switch to VLAN mode
vlan 2                          Create a VLAN by entering the VLAN ID. The VLAN ID is
                                between 1 and 4042.
vlan name 2 vlan2               Assign the VLAN 2 the name "vlan2"
vlan routing 2                  Create a virtual router interface and enable the routing
                                function
exit                            Exit from the EXEC mode
show ip vlan                    Display the virtual router interface that has been setup
           Logical
VLAN ID    Interface     IP Address       Subnet Mask        MAC Address
-------  -----------  ---------------  ---------------  -----------------
2        9/1          0.0.0.0          0.0.0.0          00:80:63:D7:F3:1F

show ip interface brief         Check the entry for the virtual router interface
```

```
                                        Netdir   Multi
Interface IP Address      IP Mask       Bcast    CastFwd
--------- --------------- --------------- -------- --------
1/5       10.0.1.1        255.255.255.0   Disable  Disable
1/6       10.0.2.1        255.255.255.0   Enable   Disable
9/1       0.0.0.0         0.0.0.0         Disable  Disable
```

`configure`	**Switch to Configuration mode**
`interface 9/1`	**Pick the VLAN interface that is setup for the virtual router. See "show ip vlan" command above.**
`ip address 10.0.3.1 255.255.255.0`	**Assign the IP address to the VLAN interface**
`routing`	**Enable routing for the interface**
`ip netdirbcast`	**Enable the transmission of the net-directed broadcast for the interface**
`exit`	**Exit Configuration mode**

`show ip interface brief`	**Check the entry for the virtual router interface**

```
                                        Netdir   Multi
Interface IP Address      IP Mask       Bcast    CastFwd
--------- --------------- --------------- -------- --------
1/5       10.0.1.1        255.255.255.0   Disable  Disable
1/6       10.0.2.1        255.255.255.0   Enable   Disable
9/1       10.0.3.1        255.255.255.0   Enable   Disable
```

`interface 1/7`	**Set the VLAN routing interface as 1/7**
`vlan participation include 2`	**Include VLAN 2 (designated as 3.2 or port# . VID)**
`vlan participation exclude 1`	**Exclude the previously set default vlan id 1**
`vlan pvid 2`	**Set the port VLAN ID to 2 i.e. the data packets which are received without a tag at the port are assigned to VLAN2 by the switch**
`exit`	**Exit configuration mode**
`interface 1/8`	**Set the VLAN routing interface as 1/7**
`vlan participation include 2`	**Include VLAN 2 (designated as 3.2 or port# . VID)**
`vlan participation exclude 1`	**Exclude the previously set default vlan id 1**
`vlan pvid 2`	**Set the port VLAN ID to 2 i.e. the data packets which are received without a tag at the port are assigned to VLAN2 by the switch**
`exit`	**Exit configuration mode**
`exit`	**Exit EXEC mode**
`show vlan 2`	**Display the VLAN 2 settings. Note settings for ports 7 and 8.**

```
VLAN ID           : 2
VLAN Name         : vlan2
VLAN Type         : Static
```

```
VLAN Creation Time: 13 days, 06:58:22 (System Uptime)

Interface   Current   Configured   Tagging
----------  --------  -----------  --------
1/1         Exclude   Autodetect   Untagged
1/2         Exclude   Autodetect   Untagged
1/3         Exclude   Autodetect   Untagged
1/4         Exclude   Autodetect   Untagged
1/5         Exclude   Autodetect   Untagged
1/6         Exclude   Autodetect   Untagged
1/7         Include   Include      Untagged
1/8         Include   Include      Untagged
1/9         Exclude   Autodetect   Untagged
1/10        Exclude   Autodetect   Untagged
1/11        Exclude   Autodetect   Untagged
1/12        Exclude   Autodetect   Untagged
1/13        Exclude   Autodetect   Untagged
1/14        Exclude   Autodetect   Untagged
1/15        Exclude   Autodetect   Untagged
1/16        Exclude   Autodetect   Untagged

show vlan port all          Check the VLAN specific settings on the ports

          Port    Acceptable   Ingress              Default
Interface VLAN ID Frame Types  Filtering    GVRP    Priority
--------- ------- ------------ ----------- ------- --------
1/1       1       Admit All    Disable     Enable     0
1/2       1       Admit All    Disable     Enable     0
1/3       1       Admit All    Disable     Enable     0
1/4       1       Admit All    Disable     Enable     0
1/5       1       Admit All    Disable     Enable     0
1/6       1       Admit All    Disable     Enable     0
1/7       2       Admit All    Disable     Enable     0
1/8       2       Admit All    Disable     Enable     0
1/9       1       Admit All    Disable     Enable     0
1/10      1       Admit All    Disable     Enable     0
1/11      1       Admit All    Disable     Enable     0
1/12      1       Admit All    Disable     Enable     0
1/13      1       Admit All    Disable     Enable     0
1/14      1       Admit All    Disable     Enable     0
1/15      1       Admit All    Disable     Enable     0
1/16      1       Admit All    Disable     Enable     0
9/1       0       Admit All    Disable     Disable    0
```

FIGURE 159 – VLAN based routing using CLI

With “Delete“, the user can delete a selected virtual router interface from the table or to reset a physical router interface‘s entry.

Note: When a VLAN router interface is deleted, the entry for the VLAN will remain in the VLAN table.

Deleting a VLAN deletes the VLAN router interface‘s entry in the router interface table.

☐ The interface IP address can be set via the Routing: Interfaces: Configuration menu as shown below.

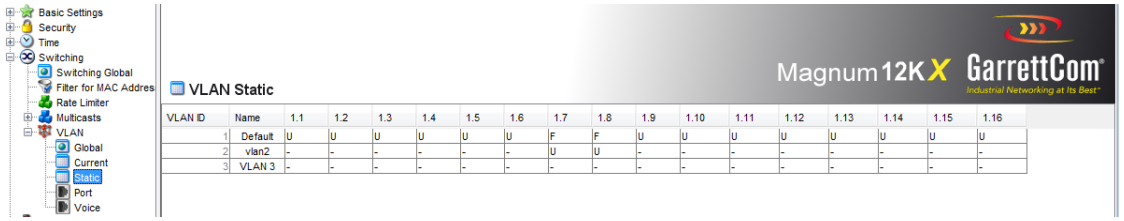


FIGURE 160 – Set the VLANs and the port memberships

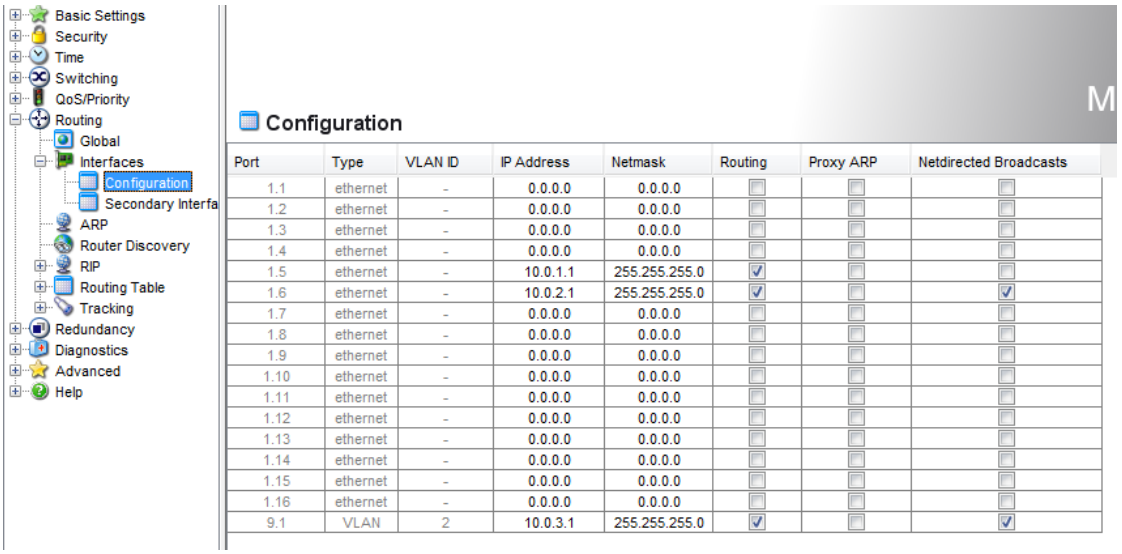


FIGURE 161 – Set the IP Addresses on interfaces.

Static Routes

In the example below, router A requires the information that it can reach the subnet 10.0.3.0/24 via the router B (next hop). It can obtain this information via a dynamic routing protocol or via a static routing entry. With this information, router A can transmit data from subnet 10.0.1.0/24 via router B into subnet 10.0.3.0/24.

Vice versa to be able to forward data of subnet 10.0.1.0/24 router B also needs an equivalent route.

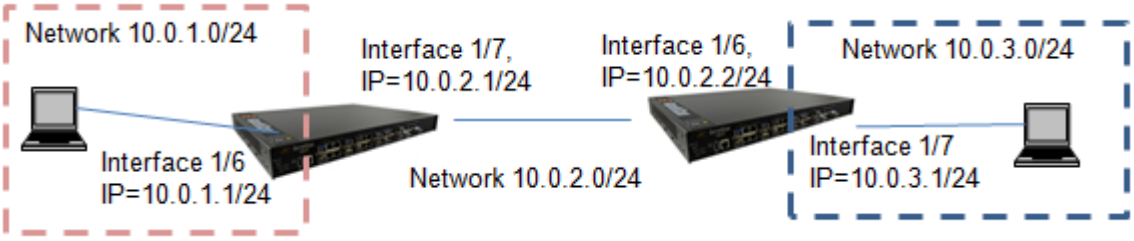


FIGURE 162 – Static Routing

Static routing can be entered for port-based and VLAN-based router interfaces.

Configuration of Static Routes

Enter a static route for router A based on the configuration of the router interface in the previous example.

```
enable                          Switch to the Privileged EXEC mode.
configure                       Switch to Configuration mode.
ip routing                      Enable the routing functionality.
ip route 10.0.3.0               Create a route to the 10.0.3.x network.
255.255.255.0 10.0.0.2
exit                            Exit the Configuration mode.
sh ip route                     Verify if the route entries have been added
      Total Number of Routes..... 3
Network         Subnet                Next Hop          Next Hop
Address         Mask         Protocol    Intf            IP Address
--------    -------------- ---------   -------------    -----------
10.0.1.0      255.255.255.0   Local       1/6             10.0.1.1
10.0.2.0      255.255.255.0   Local       1/7             10.0.2.1
10.0.3.0      255.255.255.0   Local       1/7             10.0.2.1
```

FIGURE 163 – Adding Static routes using CLI

Configure router B in the same way.

Configuration of Redundant Static Routes

To ensure a reliable connection between the two routers, the two routers can be connected with two or more lines.

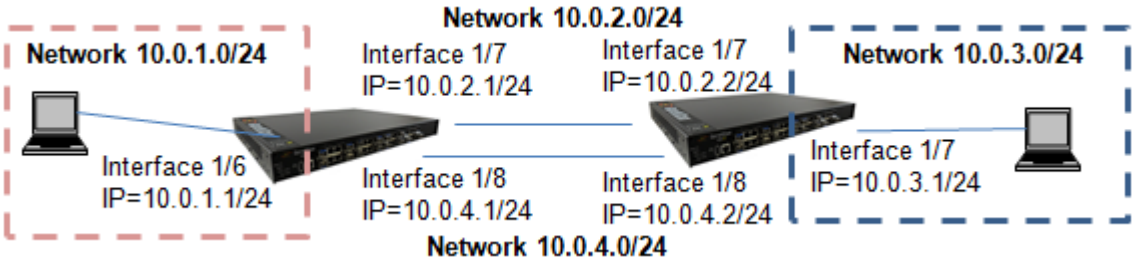


FIGURE 164 – Redundant static route

Users have the option of assigning importance (distance) to a route. If there are a number of routes to a destination, then the router chooses the route with the highest importance. If a value is not assigned for the importance during the configuration, the router takes the default value "1" for the importance. This is the highest importance.

Configure router A.

`enable`	**Switch to the Privileged EXEC mode.**
`configure`	**Switch to Configuration mode.**
`ip routing`	**Enable the routing functionality.**
`interface 1/8`	**Select interface 1/8**
`ip address 10.0.4.1 255.255.255.0`	**Set the IP address for the interface**
`routing`	**Enable routing on the interface**
`exit`	**Exit the Configuration mode**
`ip route 10.0.3.0 255.255.255.0 10.0.4.2 2`	**Create a static route for the entry. The "2" at the end of the CLI command is an important value.** **When both routes are available, the router uses the route via subnetwork 10.0.2.0/24 as the network 10.0.4.0/24 has a lower priority ("2").**
`show ip route`	**Display the IP routing information.**

```
      Total Number of Routes..... 5
Network        Subnet                Next Hop          Next Hop
Address        Mask        Protocol    Intf            IP Address
--------   -------------- ---------   -------------    -----------
10.0.1.0     255.255.255.0  Local      1/6             10.0.1.1
10.0.2.0     255.255.255.0  Local      1/7             10.0.2.1
10.0.3.0     255.255.255.0  Static     1/7             10.0.2.2
10.0.3.0     255.255.255.0  Static     1/8             10.0.4.2
10.0.4.0     255.255.255.0  Local      1/8             10.0.4.1
```

`show ip route bestroutes` **Check which routes the router is using currently**

```
Network        Subnet                Next Hop          Next Hop
Address        Mask        Protocol    Intf            IP Address
--------   -------------- ---------   -------------    -----------
10.0.1.0     255.255.255.0  Local      1/6             10.0.1.1
10.0.2.0     255.255.255.0  Local      1/7             10.0.2.1
```

```
10.0.3.0      255.255.255.0   Static      1/7             10.0.2.2
10.0.4.0      255.255.255.0   Local       1/8             10.0.4.1
Total number of routes.....................................4
```

FIGURE 165 – Adding Static routes using CLI

⋯ Configure router B in the same way.

Configuration of a Redundant Static Routes with Load Sharing

The router shares the load between the two routes (load sharing), when the routes have the same importance (distance). Follow the steps for adding routes discussed above. Modify the router statement priority as shown below.

```
ip route 10.0.3.0 255.255.255.0 10.0.2.2 2
```
Assign the route weight "2" to the route i.e. make the weight of the two routes the same.

```
show ip route
```
Display the IP routing information.

```
      Total Number of Routes..... 4
Network         Subnet                  Next Hop          Next Hop
Address         Mask         Protocol    Intf             IP Address
--------    -------------- ---------    -------------     -----------
10.0.1.0      255.255.255.0   Local       1/6             10.0.1.1
10.0.2.0      255.255.255.0   Local       1/7             10.0.2.1
10.0.3.0      255.255.255.0   Static      1/7             10.0.2.2
                                          1/8             10.0.4.2
10.0.4.0      255.255.255.0   Local       1/8             10.0.4.1
```

```
show ip route bestroutes
```
Check which routes the router is using currently

```
Network         Subnet                  Next Hop          Next Hop
Address         Mask         Protocol    Intf             IP Address
--------    -------------- ---------    -------------     -----------
10.0.1.0      255.255.255.0   Local       1/6             10.0.1.1
10.0.2.0      255.255.255.0   Local       1/7             10.0.2.1
10.0.3.0      255.255.255.0   Static      1/7             10.0.2.2
                                          1/8             10.0.4.2
10.0.4.0      255.255.255.0   Local       1/8             10.0.4.1
Total number of routes.....................................4
```

FIGURE 166 – Adding Static routes using CLI

Static route tracking

Description of the static route tracking function

With static routing, if there are a number of routes to a destination, the router chooses the route with the highest importance. The router detects an existing route by the state of the router interface. While connection L 1 on the router interface may be fine, the connection to remote router B at location L 2 may be interrupted. In this case, the router continues transmitting via the interrupted route.

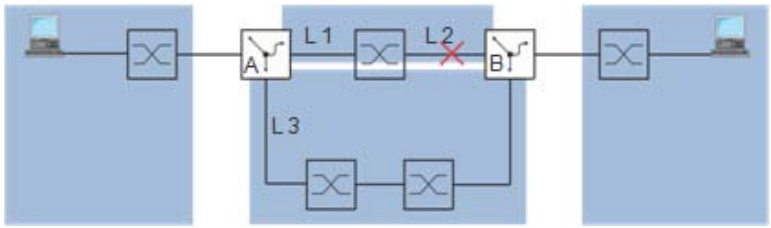


FIGURE 167 – Example of static route tracking

With the static route tracking function, the router uses a tracking object such as a ping tracking object to detect the connection interruption. The active static route tracking function then deletes the interrupted route from the current routing table. If the tracking object returns to the “up” state, the router enters the static route in the current routing table again.

Application Example for the Static Route Tracking Function

The figure shows an example of the static route tracking function: Router A monitors the best route via L 1 with ping tracking. If there is a connection interruption, router A transmits via redundant connection L 3. The following is known:

Parameter	Router A	Router B
IP address interface (IF) 1.1	10.0.4.1	
IP address interface (IF) 1.2	10.0.2.1	10.0.4.2
IP address interface (IF) 1.3		10.0.2.53
IP address interface (IF) 1.4	10.0.1.112	
IP address interface (IF) 2.2		10.0.5.1
Netmask	255.255.255.0	255.255.255.0

Table 32: Static Route Example

Prerequisites for further configuration:

- The IP parameters of the router interface are configured.
- The router function is activated globally and at the ports/router interface.
- Ping tracking at interface 1.2 of router A is configured

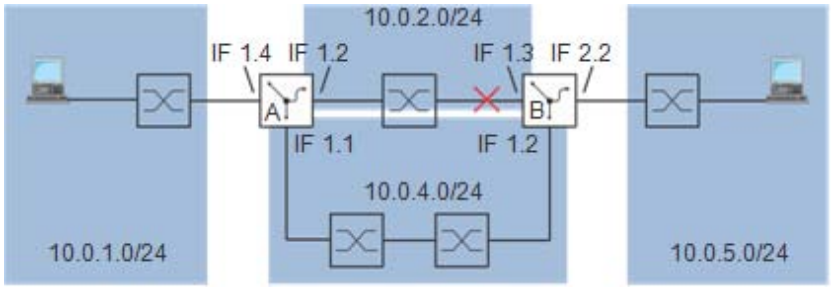


FIGURE 168 – Configuring static route tracking

Enter the two routes to destination network 10.0.5.0/24 in the static routing table of router A.

Select the dialog `Routing:Routing Table:Static`. Click on “Create Entry”.

Enter the data for the first static route:

“Destination Network”	10.0.5.0
“Destination Netmask”	255.255.255.0
“Next Hop”	10.0.2.53
“Track ID”	21

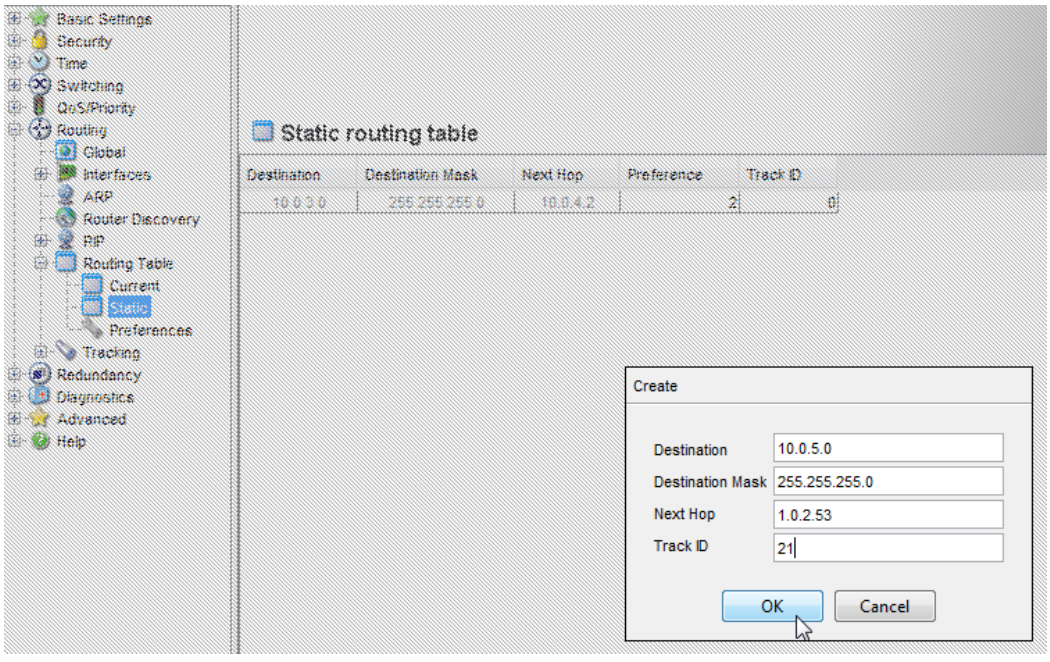


FIGURE 169 – Set route entry for tracking

Click on “Create Entry”.

Enter the data for the first static route:

“Destination Network”	10.0.5.0
“Destination Netmask”	255.255.255.0
“Next Hop”	10.0.2.53
“Track ID”	0

… Click on "OK"

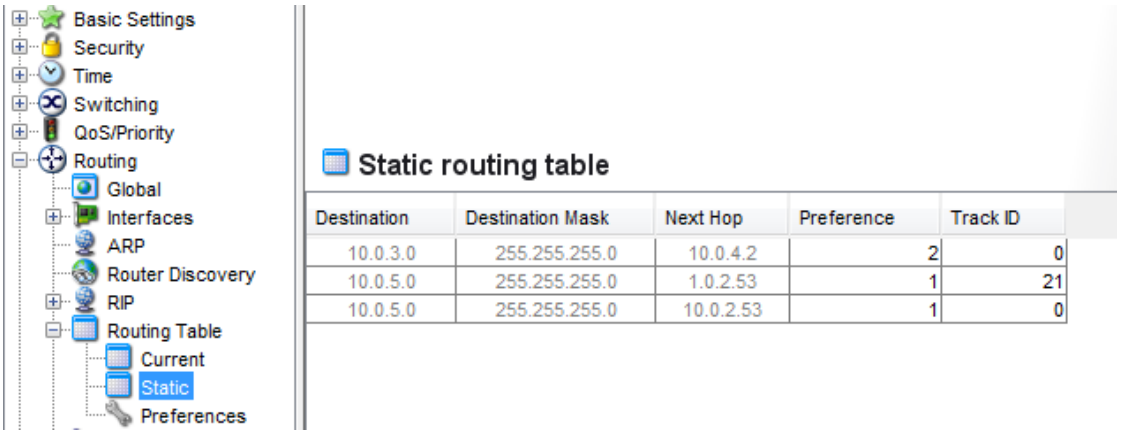


FIGURE 170 – Routing table after the entries are created.

```
enable                                  Switch to the Privileged EXEC mode.
configure                               Switch to Configuration mode.
ip route 10.0.5.0                       Create the static route entry with preference 1 and track
255.255.255.0 10.0.2.53.1               ID of 21.
track 21
ip route 10.0.5.0                       Create the static route entry with preference 2.
255.255.255.0 10.0.4.2 2
exit                                    Exit the privilege EXEC mode
show ip route                           Display the IP routes
Total Number of Routes..................... 3

   Network          Subnet                    Next Hop    Next Hop
   Address           Mask         Protocol     Intf     IP Address
--------------- --------------- ------------  ------  ---------------
10.0.1.0        255.255.255.0   Local         1/5       10.0.1.1
10.0.2.0        255.255.255.0   Local         1/6       10.0.2.1
10.0.5.0        255.255.255.0   Static        1/6       10.0.2.53
```

FIGURE 171 – Adding Static routes using CLI

On router B, create a ping tracking object with the track ID, for example 22, for IP address 10.0.2.1. Enter the two routes to destination network 10.0.1.0/24 in the static routing table of router B.

Destination Network	Destination Netmask	Next Hop	Preference	Track ID
10.0.1.0	255.255.255.0	10.0.2.1	1	22
10.0.1.0	255.255.255.0	10.0.4.1	2	

Table 33: Static routing entries for router B

Chapter 18

Tracking

The tracking function provides the option of monitoring certain objects, such as the availability of an interface. A special feature of this function is that it forwards an object status change to an application, e.g. VRRP, which previously registered as an interested party for this information.

Tracking can monitor the following objects:

- Link status of an interface (interface tracking)
- Accessibility of a device (ping tracking)
- Result of logical connections of tracking entries (logic tracking)

An object can have the following statuses:

- up (OK)
- down (not OK)

The definition of "up" and "down" depends on the type of the tracking object (e.g. interface tracking).

Tracking can forward the state changes of an object to the following applications:

- VRRP
- Static routing

Interface tracking

With interface tracking the Switch monitors the link status of:

- physical ports
- link aggregation interfaces (interfaces 8.x)
- VLAN router interfaces (interfaces 9.x)

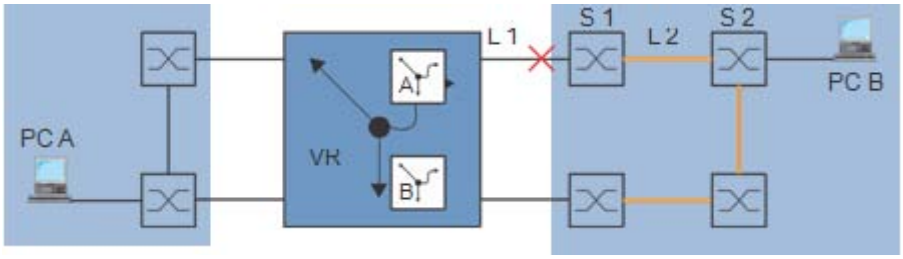


FIGURE 172 – Monitoring a line with interface tracking

Ports/interfaces can have the following link statuses:

- interrupted physical link (link down) and
- existing physical link (link up).

A link aggregation interface has link status “down” if the link to all the participating ports is interrupted.

A VLAN router interface has link status “down” if the link is interrupted from all the physical ports/link aggregation interfaces that are members of the corresponding VLAN.

Setting a delay time enables the insertion of a delay before informing the application about an object status change.

An interface tracking object is given the “down” status if the physical link interruption remains for longer than the “link down delay” delay time.

An interface tracking object is given the “up” status if the physical link holds for longer than the “link up delay” delay time.

State on delivery: delay times = 0 seconds. This means that if a status changes, the registered application is informed immediately. The “link down delay” and “link up delay” delay times can be set independently of each other in the range from 0 to 255 seconds. An interface tracking object can be defined for each interface.

Ping tracking

With ping tracking, the Magnum 12KX uses ping requests to monitor the link status to other devices.

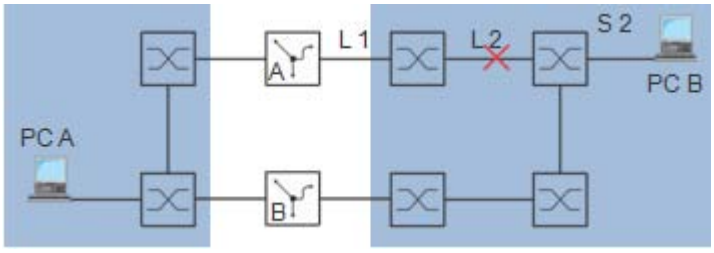


FIGURE 173 – Monitoring a line with ping tracking

The Magnum 12KX sends ping requests to the device with the IP address that was entered in the “IP Address” column. The “Ping Interval” column allows the user to define the frequency for sending ping requests, and thus the additional network load. If the response comes back within the time entered in the “Ping Timeout” column, this response is a valid “Ping response received”. If the response comes back after the time entered in the “Ping Timeout” column, or not at all, this response is evaluated as “No ping response”.

Ping tracking objects can have the following statuses:

- the number of “No ping responses” is greater than the number entered (down) and
- the number of “Ping responses received” is greater than the number entered (up).

Entering a number for lost packets or received ping responses enables the user to set the sensitivity of the ping behavior of the device. The Magnum 12KX informs the application about an object status change.

Ping tracking enables the user to monitor the accessibility of defined devices. As soon as a monitored device can no longer be accessed, the Magnum 12KX can choose to use an alternative path.

Select the dialog `Routing:Routing Table:Static`. Click on “Create Entry”.

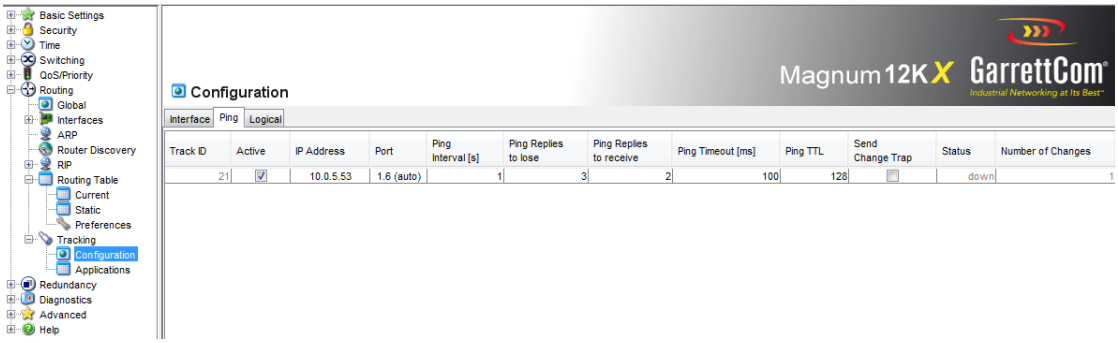


FIGURE 174 – Ping Tracking dialog

Logical tracking

Logical tracking enables the logical linking of multiple tracking objects with each other and thus perform relatively complex monitoring tasks. Logical tracking can be used for example to monitor the link status for a network node to which redundant paths lead.

The Magnum 12KX provides the following options for a logical link:

- AND
- OR

For a logical link, up to 8 operands can be combined with one operator.

Logical tracking objects can have the following statuses:

- The result of the logical link is incorrect (down).
- The result of the logical link is correct (up).

When a logical link delivers the result “incorrect”, the Magnum 12KX can choose to use an alternative path.

Configuring the tracking

The tracking can be configured by setting up tracking objects. The following steps are required to set up a tracking object:

- Enter the tracking object ID number (track ID).
- Select a tracking type, e.g. interface.
- Depending on the track type, enter additional options such as “port” or “link up delay” in the interface tracking.

Note: The registration of applications (e.g. VRRP) to which the tracking function reports status changes is performed in the application itself.

Configuring interface tracking

Set up interface tracking at port 1.1 with a link down delay of 0 seconds and a link up delay of 3 seconds.

In the `Routing:Tracking:Configuration` dialog, click on “Wizard” at the bottom right.
Select type as Interface
Enter the values as needed. For this example use

Interface	7
Track id of 1. Module Port:	1.1
Link up delay	3
Link down delay	0

Click on “Finish” to leave the Wizard and save the entry temporarily in the configuration.

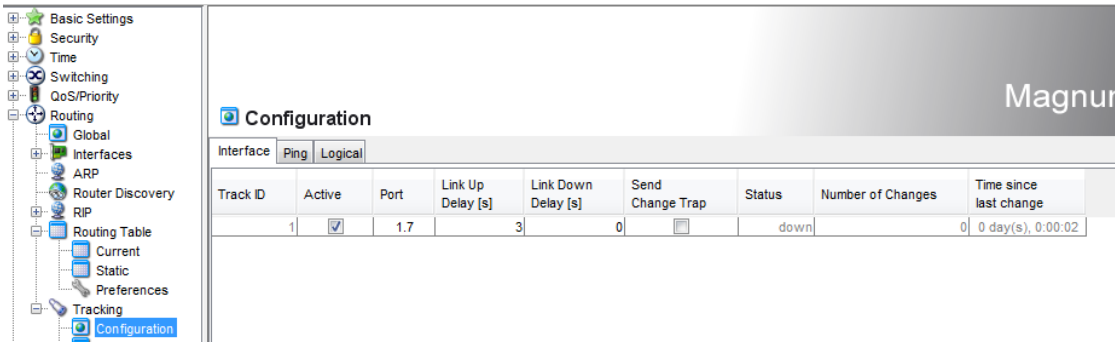


FIGURE 175 – Link Tracking dialog

```
enable                          Switch to the Privileged EXEC mode.
configure                       Switch to Configuration mode.
track 1 interface 1/7           Enter the tracking information. Note - if the tracking ID
link-down-delay 0               already exists, it is overwritten.
link-up-delay 3

Tracking ID 1 already exists.
  Temporarily disabled for modification.
  Target interface set to 1/7
  Link Down Delay for target interface set to 0 sec
  Link Up Delay for target interface set to 3 sec
Tracking ID 1 activated

exit                            Exit the privilege EXEC mode.
show track                      Display the tracking information. Note - this command
                                displays all the tracking information setup.
```

```
Interface Tracking
                  Link Delay                    No. of
  ID Type  Intf   Down   Up    Status  Mode    Changes Time since last change
 --- ----- ----- ------ ------ ------ ------- ------- ----------------------
   1  Intf 1/7     0s     3s    DOWN  Enable        0   0 day(s), 00:03:37

Ping Tracking
                                                 No. of
  ID Type   IP Address       Intvl  Status  Mode   Changes Time since last change
 --- ----- ---------------- ------ ------ ------- ------- ----------------------
  21  Ping        10.0.5.53     1s    DOWN  Enable        1   0 day(s), 00:14:27
```

FIGURE 176 – Adding Static routes using CLI

Application example for ping tracking

While the interface tracking monitors the directly connected link, the ping tracking monitors the entire link to Switch S2.

Set up ping tracking at port 1.7 for IP address 10.0.2.53 with the preset parameters. In the `Routing:Tracking:Configuration` dialog, click on “Wizard” at the bottom right.

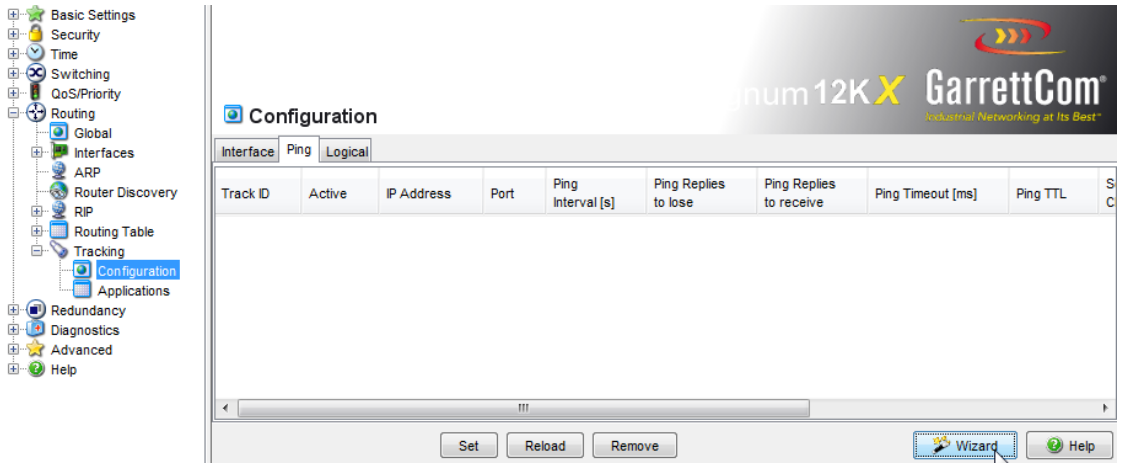


FIGURE 177 – Adding Ping Tracking via the Wizard. Make sure to click on the Ping tab.

Enter the values in the Wizard.

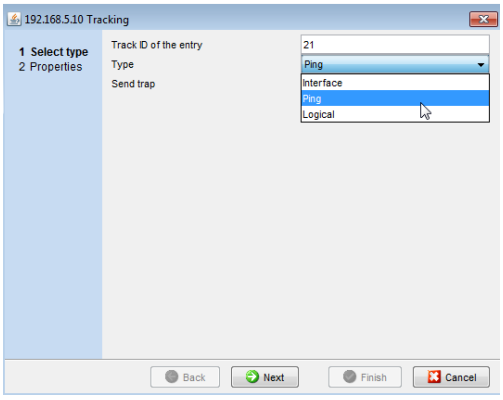


FIGURE 178 – Enter values in the Wizard. Select the type as "Ping".

Enter the values for the Properties as step 2 of the Wizard and click on Finish when done.

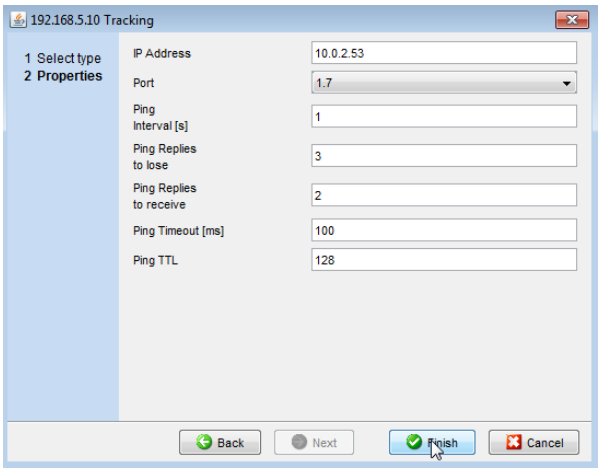


FIGURE 179 – Enter the values for the Properties and click "Finish" when done.

When completed, the entry shows up on the Ping tab.

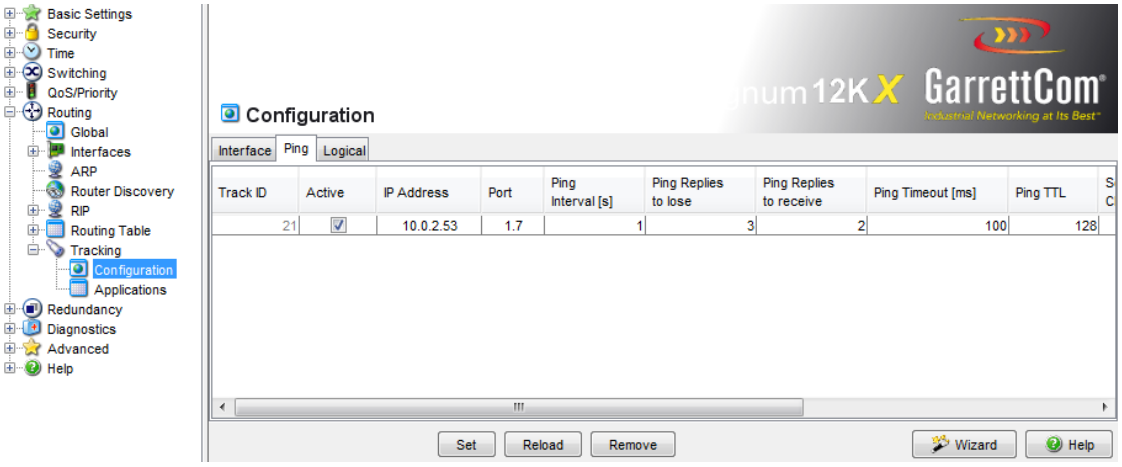


FIGURE 180 – Successful entry for Ping tracking.

```
enable                          Switch to the Privileged EXEC mode.
configure                       Switch to Configuration mode.
track 21 ping 10.0.2.53         Enter the tracking information. Note - if the tracking ID
interface 1/7 interval 1        already exists, it is overwritten.
miss 3 success 2 timeout 100
Tracking ID 21 already exists.
  Temporarily disabled for modification.
  Target IP address set to 10.0.2.53
  Interface used for sending pings to target set to 1/7
  Ping Interval for target set to 1 sec
  Max. no. of missed ping replies from target set to 3
  Min. no. of received ping replies from target set to 2
  Timeout for ping replies from target set to 100 ms
Tracking ID 21 activated
exit                            Exit the Privileged EXEC mode
show track                      Display the currently configured tracking

Ping Tracking
                                                        No. of
 ID Type   IP Address       Intvl  Status  Mode   Changes Time since last change
--- ----- ---------------- ------ ------ ------- ------- ---------------------
 21  Ping  10.0.2.53        1s     DOWN    Enable    1     0 day(s), 00:01:17
```

FIGURE 181 – Adding Ping tracking via CLI.

Application example for logical tracking

The figure shows an example of monitoring the connection to a redundant ring. By monitoring lines L 2 and L 4, a line interruption can be detected from router A to the redundant ring. With a ping tracking object at port 1.1 of router A, monitor the connection to Switch S2. With an additional ping tracking object at port 1.1 of router A, monitor the connection to Switch S4. Only the OR link of both ping tracking objects delivers the precise result that router A has no connection to the ring. One ping tracking object for Switch S3 could indicate an interrupted connection to the redundant ring, but in this case there could be another reason for the lack of a ping response from Switch S3. For example, there could be a power failure at Switch S3.

The following is known:

Parameter	Value
Operand No. 1 (track ID)	21
Operand No. 2 (track ID)	22

Prerequisites for further configuration:

- The ping tracking objects for operands 1 and 2 are configured.

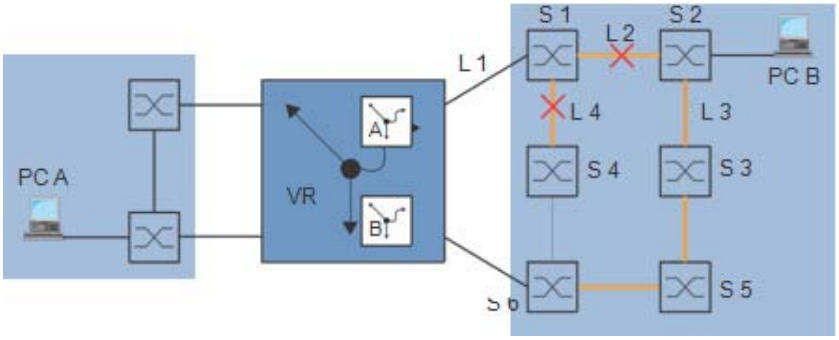


FIGURE 182 – Monitoring the accessibility of a device in a redundant ring

Set up ping tracking at port 1.7 for IP address 10.0.2.53 with the preset parameters. In the `Routing:Tracking:Configuration` dialog, click on "Wizard" at the bottom right.

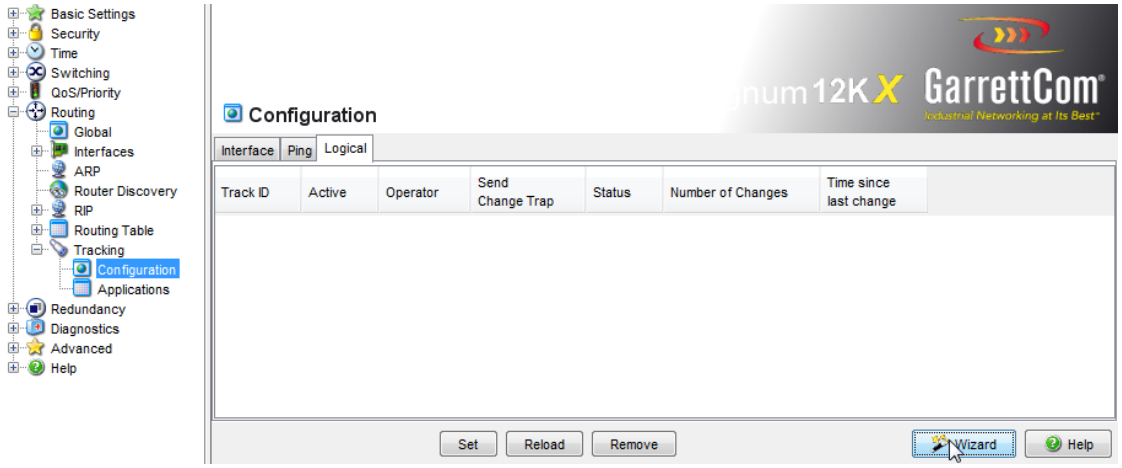


FIGURE 183 – Adding Ping Tracking via the Wizard. Make sure to click on the Logical tab.

Enter the values in the Wizard.

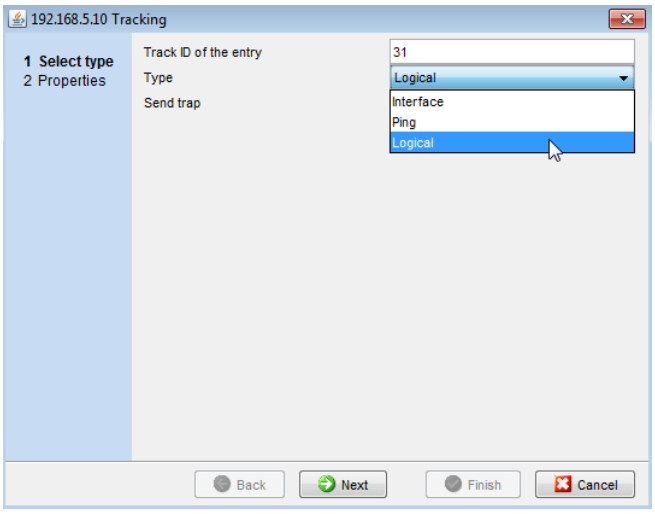


FIGURE 184 – Enter values in the Wizard. Select the type as "Logical".

Enter the values for the Properties as step 2 of the Wizard and click on Finish when done.

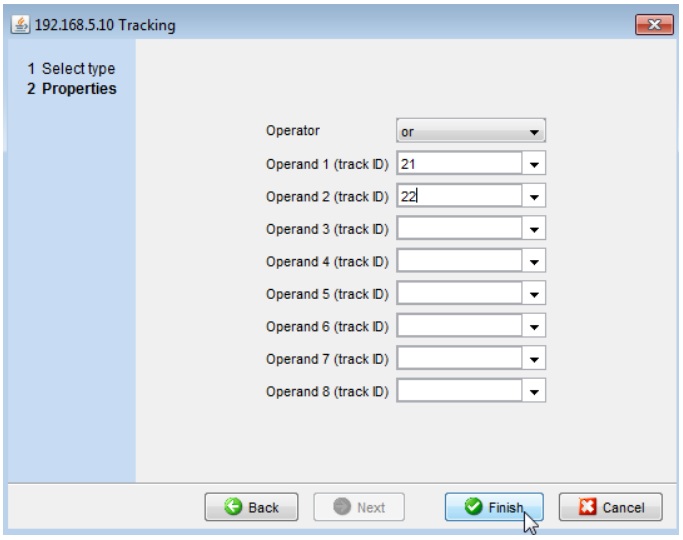


FIGURE 185 – Enter the values for the Properties as shown and click "Finish" when done.

When completed, the entry shows up on the Logical tab.

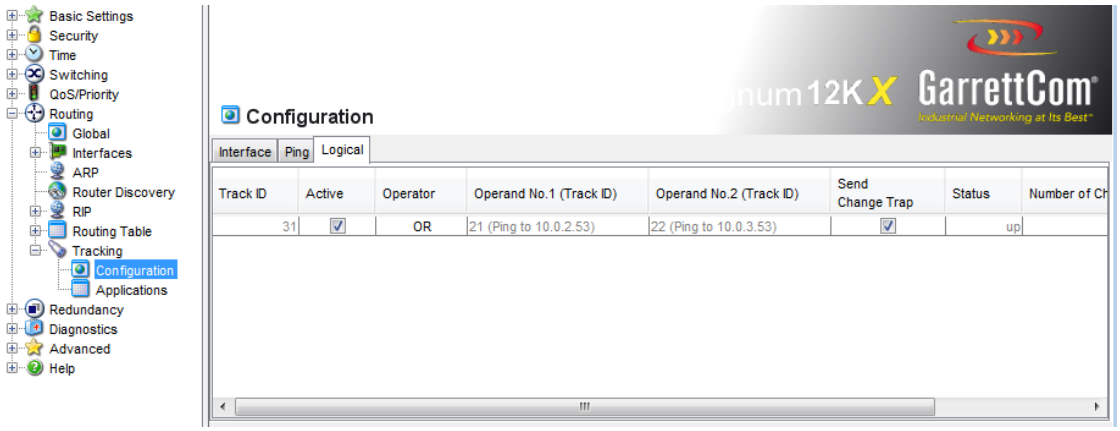


FIGURE 186 – Successful entry for Logical tracking.

```
enable                          Switch to the Privileged EXEC mode.
configure                       Switch to Configuration mode.
track 31 logical or 21 22       Enter the tracking information. Note - if the tracking ID
                                already exists, it is overwritten.
Tracking ID 31 already exists.
  Temporarily disabled for modification.
  Tracking type set to Logical
  Logical Operator set to or
  Logical Instance 22 included
  Logical Instance 21 included
Tracking ID 31 activated
exit                            Exit the Privileged EXEC mode
show track                      Display the currently configured tracking

Ping Tracking
                                                          No. of
  ID Type   IP Address       Intvl  Status  Mode    Changes Time since last change
 --- ----- ---------------- ------ ------ ------- ------- ----------------------
  21  Ping   10.0.2.53        1s   DOWN    Enable    1      0 day(s), 00:03:35
  22  Ping   10.0.3.53        1s   DOWN    Enable    1      0 day(s), 00:03:19

Logical Tracking
                                              No. of
  ID Type   Instances          Status  Mode   Changes Time since last change
 --- ----- ------------------- ------ ------- ------- ----------------------
  31  OR   21,22                DOWN  Enable     0      0 day(s), 00:00:24
```

FIGURE 187 – Adding logical tracking via CLI.

Finally, do not forget to save the changes.

Chapter 19

VRRP/HiVRRP

Many edge devices usually give the option of entering a default gateway for transmitting data packets in external subnetworks. Here the term “Gateway” applies to a router by means of which the terminal device can communicate in other subnetworks.

If this router fails, the edge device cannot send any more data to external subnetworks. To allow for a secondary router to act as a default gateway is enabled by VRRP, the Virtual Router Redundancy Protocol. VRRP is a type of “gateway redundancy” capability. VRRP describes a process that groups multiple physical routers as one virtual router. Edge devices always use the IP address of the virtual router, and VRRP ensures that a physical routers belonging to the virtual router takes over the data transmission, should one of the routers were to go down. VRRP is not restricted ot one device. VRRP can be setup across different physical devices. Even if a physical router fails, VRRP ensures that another router takes over the function as part of the virtual router.

VRRP has typical switching times of 3 to 4 seconds when a physical router fails. VRRP is thus slower than L2 redundancy capabilities such as RSTP etc. Certain applications such as Voice over IP, Video over IP, industrial controllers, etc., may find this long switch over time as non acceptable. To overcome these limitations, Belden has developed an extension to HRRP.

Belden has developed a proprietary enhancements to VRRP via the Hirschmann Virtual Router Redundancy Protocol (HiVRRP). With the appropriate configuration, HiVRRP guarantees maximum switching times of 400 milliseconds. Thanks to this guaranteed switching time, HiVRRP enables the use of “gateway redundancy” in time-critical applications. Applications which require switch over times of less than one second for VRRP should use the HiVRRP protocol. By using this application, a user can improve the network availability with this form of “gateway redundancy”.

VRRP

All the routers within a network on which VRRP is active specify among themselves which router is to be the master. This router contains the IP and MAC address of the virtual router. All the devices in the network that have entered this virtual IP address as the default gateway use the master as the default gateway.

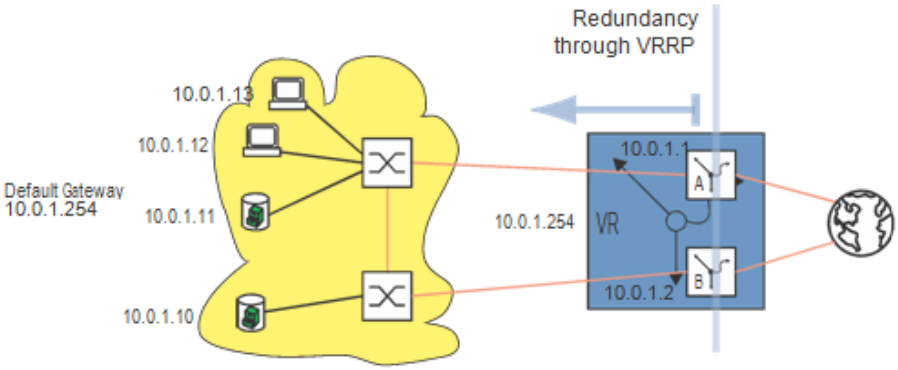


FIGURE 188 – Illustration of the virtual router

If the master fails, then the remaining routers use the VRRP to specify a new master. This router then takes over the IP and MAC address of the virtual router. Thus the devices find their route via their default gateway, as before. The devices always only see the master with the virtual MAC and IP addresses, regardless of which router is actually behind this virtual address. The virtual router IP address is assigned by the administrator. The VRRP specifies the virtual MAC address with: 00:00:5e:00:01:<VRID>. The first 5 octets form the fixed part in accordance with RFC-2338. The last octet is the virtual router ID (VRID). It is a number between 1 and 255. On the basis of this, the administrator can define 255 virtual routers within a network.

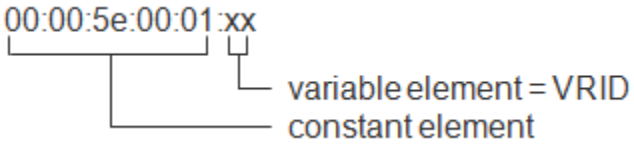


FIGURE 189 – Virtual MAC address

The VRRP router sends IP Multicast messages to the IP Multicast address 224.0.0.18 in order to determine the master. The router with the highest VRRP priority becomes the master. The VRRP priority is specified by the administrator. If the VRRP priorities are the same, then the highest IP interface address of the VRRP routers is decisive. If the virtual IP address is the same as the IP address of a router interface, then this router is the IP address owner. VRRP sets the VRRP priority of an IP address owner to the value 255 and thus declares it the master. If there is no IP address owner, then VRRP declares the router with the highest VRRP priority the master.

The master regularly sends IP Multicast messages (default: 1 s) to the other VRRP routers in order to signal that it is ready for operation. If this message does not appear three times in a row, then the VRRP router with the highest remaining VRRP priority declares itself the new master.

1. The IP address owner as it has the highest priority (255) by definition is the master.
2. The VRRP router with the highest VRRP priority is the master.
3. If the priorities are the same, the VRRP router with the highest IP address is the master.

Table 34: Determining the master for VRRP

VRRP terms

- Virtual router: A virtual router is a router or group of routers that act as the default gateway in a

network and use the Virtual Router Redundancy Protocol.

- VRRP router: A VRRP router is a router that uses VRRP. It can be part of one or more virtual routers.
- Master router: The master router is the router within the virtual router that is currently responsible for forwarding data packets and responding to ARP queries. The master router periodically sends messages (advertisements) to the other VRRP routers (backup routers) to inform them about its existence.
- IP address owner: The IP address owner is the VRRP router whose IP address is identical to the IP address of the virtual router. By definition, it has the highest VRRP priority (255) and is thus automatically the master router.
- Backup router: The backup router is a VRRP router that is not the master router. The backup router is ready to take over the master role, should the master fail.
- VRRP priority: The VRRP priority is a number between 1 and 255. It is used to determine the master router. The value 255 is reserved for the IP address owner.
- VRID: The VRID (virtual router ID) uniquely identifies a virtual router.
- Virtual router MAC address: The virtual router MAC address is the MAC address of the virtual router
- Virtual router IP address: The virtual router IP address is the IP address of the virtual router.
- Advertisement interval: The advertisement interval describes the frequency with which the master router sends its existence message (advertisement) to all the VRRP routers of its virtual router. The values for the advertisement interval are between 1 and 255 seconds. The default value is 1 second.
- Skew time: The skew time is the time, dependent on the VRRP priority, that specifies the time when the backup router names itself the master router.
  Skew time = ((256 - VRRP priority) / 256) * 1 second
- Master down interval: The master down interval specifies the time when the backup router names itself the master router.
  Master down interval = 3 * advertisement interval + skew time

Configuration of VRRP

- The configuration of VRRP requires the following steps:
- Switch on routing globally (if this has not already been done).
- Switch on VRRP globally.
- Configure port assign IP address and network mask.
- Switch on VRRP at the port.
- Create virtual router ID (VRID), because there exists the option of activating a multiple virtual routers for each port.
- Assign virtual router IP address.
- Switch on virtual router.
- Assign VRRP priority.

Set up VRRP for ports 1/3 and 1/4 the preset parameters. Use the `Redundancy:VRRP/HiVRRP:Configuration` dialog, click on “Wizard” at the bottom right.

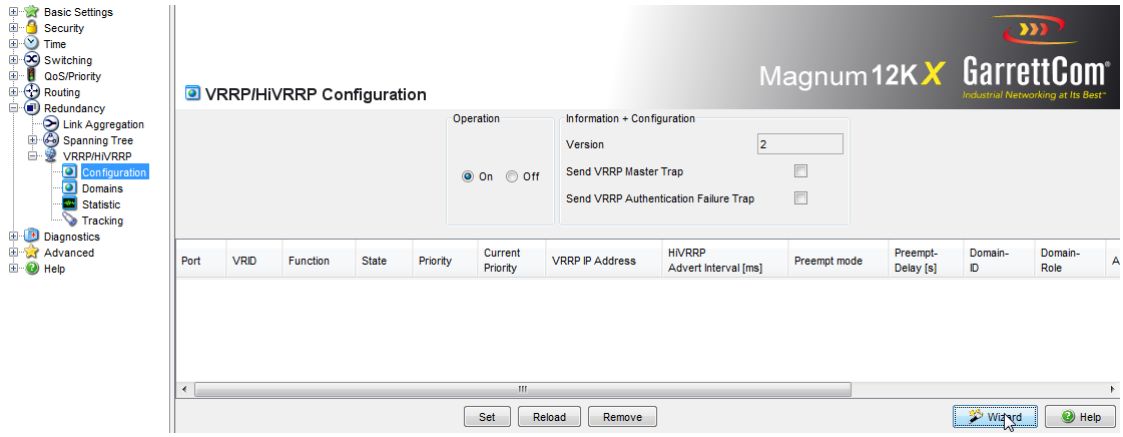


FIGURE 190 – Adding VRRP via the Wizard. Make sure the Operation for VRRP is set to "On". If VRRP configuration changes should generate a trap, make sure to check the Trap boxes as well.

Enter the values in the Wizard as described in the steps above.

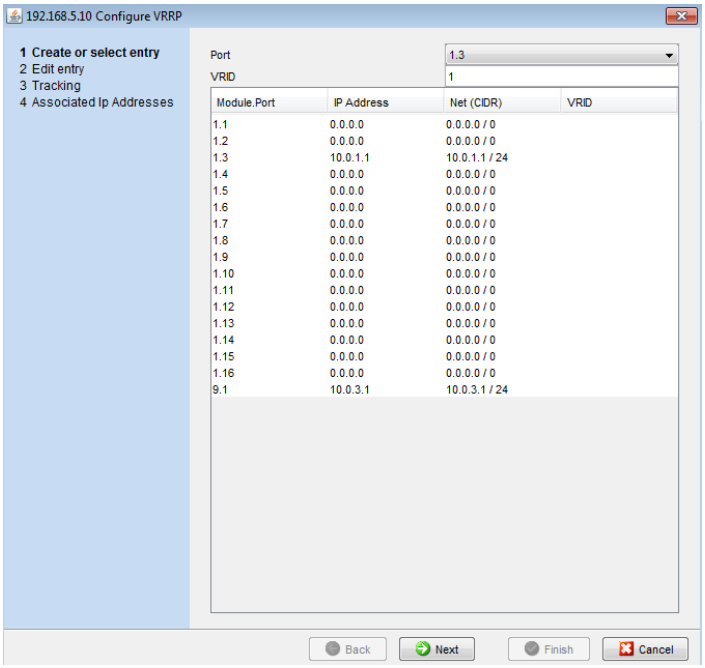


FIGURE 191 – Select VRRP ID and the port the VRRP is setup on.

Enter the values for the Properties as step 2 of the Wizard and click on Finish when done.

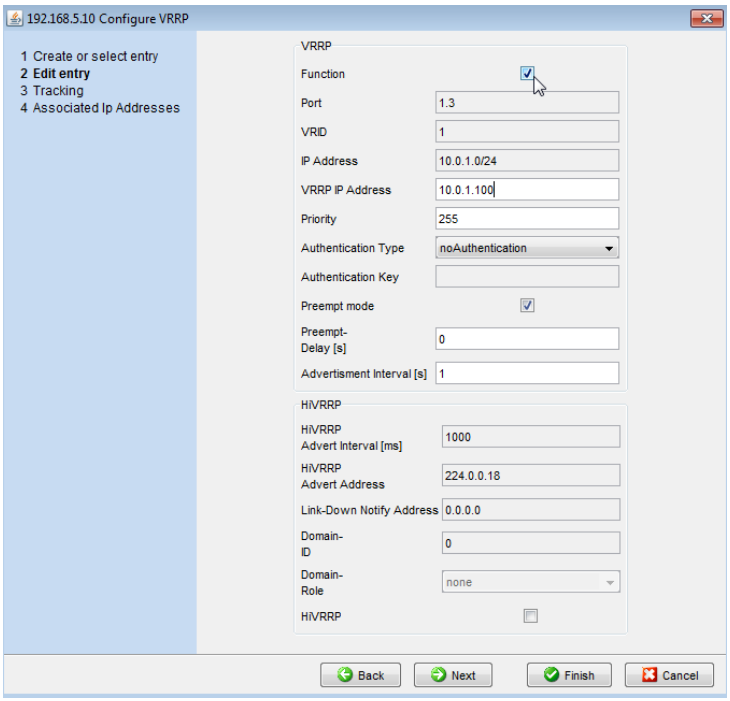


FIGURE 192 – Enter the values for the interface. Make sure the VRRP Function box is checked. If needed, the authentication string (password) can also be added. Click "Finish" when done. Repeat similarly for the other router.

`enable`	**Switch to the Privileged EXEC mode.**
`configure`	**Switch to Configuration mode.**
`ip routing`	**Enable routing**
`ip vrrp`	**Enable VRRP**
`interface 1/3`	**Select the interface for setting up VRRP**
`ip address 10.0.1.1 255.255.255.0`	**Set the IP parameters for the interface**
`routing`	**Enable routing for the interface**
`ip vrrp 1`	**Setup first VRRP id for this interface**
`ip vrrp 1 mode`	**Enable VRRP on this interface**
`ip vrrp 1 ip 10.0.1.100`	**Assign Virtual Router 1 the IP address. By default, this becomes the primary address.**
`ip vrrp 1 priority 200`	**Set the Virtual Router VRRP priority of 200**
`exit`	**Exit from the configuration for the VRRP for the interface**
`ip vrrp domain 1 send-member-advertisments`	**Setup the VRRP Domain. The "send-member-advertisements" configures whether the members of the domain send advertisements on their own. This can be used to react to domain failures.**

`ip vrrp trap new-master`	**Enable sending trap if this router becomes the new master. The same command is also used to disable the trap.**

Configure additional ports as needed. Also configure other Virtual routers following the same syntax.
The `show ip vrrp interface brief` command displays the status of the VRRP setup.

FIGURE 193 – Adding VRRP via CLI.

HiVRRP

HiVRRP provides a number of mechanisms for shortening the switching times or reducing the number of Multicasts:

- shorter advertisement intervals
- link-down notification
- preempt delay
- Unicast advertisement
- domains

In compliance with RFC-2338, the master sends IP Multicast messages (advertisements) at intervals of one second to the other VRRP routers. Only if this message does not appear three times do the remaining routers select a new master. VRRP has typical switching times of 3 to 4 seconds.

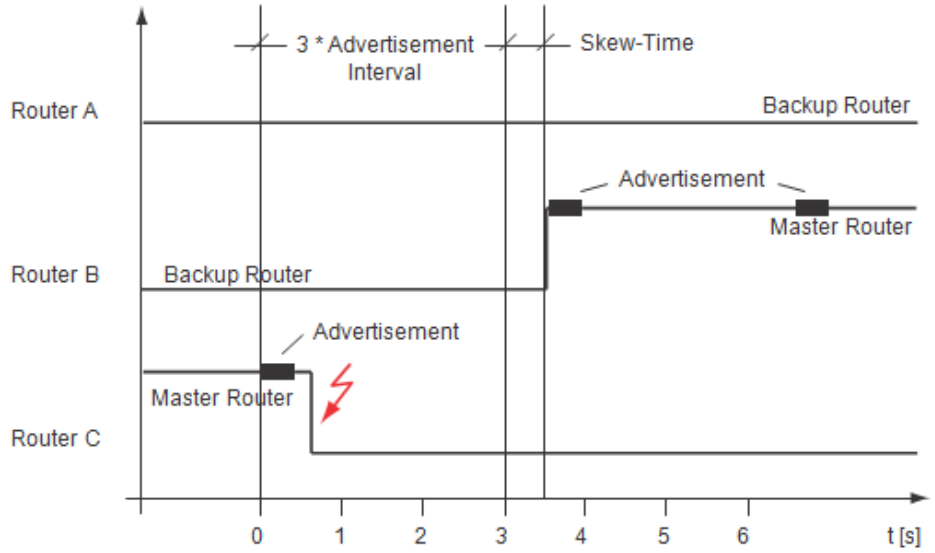


FIGURE 194 – Master router <-> backup router switching times according to RFC-2338
VRRP priority router A = 64
VRRP priority router B = 128
VRRP priority router C = 254

To be able to achieve faster switching times, Hirschmann provides HiVRRP so that the cycle for sending the IP Multicast message can be shortened to as little as 0.1 seconds. Users can thus achieve switching times that are up to ten times as fast. The router supports up to 16 VRRP router interfaces with this shortened sending cycle.

- HiVRRP skew time

The HiVRRP skew time is the time, dependent on the VRRP priority, that specifies the time when the HiVRRP backup router names itself the
HiVRRP master router. HiVRRP skew time =
(256 - VRRP priority) / 256 * advertisement interval
Times shown in milliseconds

- HiVRRP master down interval
  The HiVRRP master down interval specifies the time when the HiVRRP
  backup router names itself the HiVRRP master router. HiVRRP master down interval =
  3 * advertisement interval + HiVRRP skew time
  Times shown in milliseconds

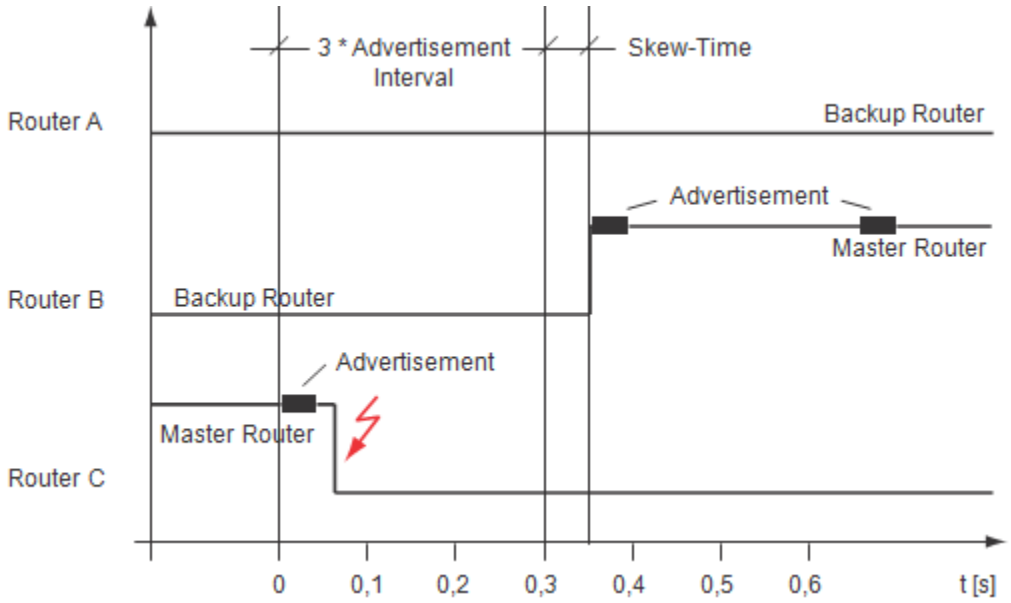


FIGURE 195 – Master router <-> backup router switching times according to HiVRRP
VRRP priority router A = 64
VRRP priority router B = 128
VRRP priority router C = 254

Another option provided by HiVRRP for shortening the switching times dramatically is the link-down notification. This function can be used when the virtual router consists of two VRRP routers. As two VRRP routers are participating, it is sufficient to send the link-down notification in the form of a Unicast message. In contrast to the Multicast message, the Unicast message travels beyond the boundaries of the subnetwork. This means that if the link is down to the subnetwork, the link-down notification can also travel via another subnetwork to reach the second router of the virtual router. As soon as HiVRRP detects that the link is down, it sends the link-down notification to the second router via a different route. The second router takes over the master function immediately after receiving the link-down notification.

In the preempt mode, the backup router can take over the master function from the master router as soon as the backup router receives an advertisement from the master router for which the VRRP priority is lower than its own. Thus the preempt mode, in collaboration with VRRP tracking (see page 66), can enable a switch to a better router. However, dynamic routing procedures take a certain amount of time to react to changed routes and refill their routing table. To avoid the loss of packets during this time, delayed switching (preempt delay) from the master router to the backup router enables the dynamic routing procedure to fill the routing tables.

HiVRRP provides an additional advantage for networks with devices that have problems with higher volumes of Multicasts. Instead of sending advertisements in the form of Multicasts, HiVRRP can send the advertisements in the form of Unicast data packets (VRRP destination address) when using up to two

HiVRRP routers.

Note: To avail of the advantages of HiVRRP, only use VRRP routers equipped with the HiVRRP function from Hirschmann as the virtual router.

HiVRRP Domains

In large, flat network structures, HiVRRP domains enable the user to

- switch over all HiVRRP routers very quickly in the case of redundancy
- use the available bandwidth more effectively
- configure more than 16 VRRP router interfaces for each router using HiVRRP
- operate Multicast-sensitive terminal devices in large HiVRRP networks

A HiVRRP instance is a router interface configured as HiVRRP with functions that HiVRRP contains. In a HiVRRP domain combine multiple HiVRRP instances of a router into one administrative unit. Nominate one HiVRRP instance as the supervisor of the HiVRRP domain. This supervisor regulates the behavior of all HiVRRP instances in its domain.

- The supervisor sends its advertisements on behalf of all HiVRRP instances in its domain.
- The supervisor puts itself and the other HiVRRP instances together into the master role or the backup role.

See fig. below for an example of a flat network structure. All cross-VLAN data streams pass through the ring.

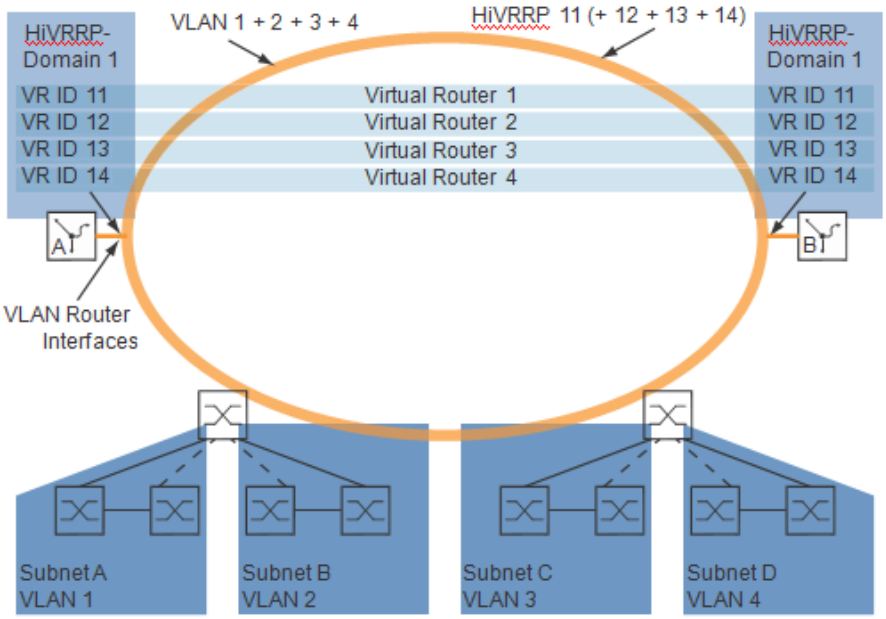


FIGURE 196 – Example of how a HiVRRP domain is used

Configuration of HiVRRP domains

The configuration of HiVRRP domains consists of the following steps:

- Create VLANs
- Configure VLAN router interfaces
- Assign the IP addresses to the router interfaces
- Configure HiVRRP instances
  - Activate VRRP instance (all instances)
  - Assign IP address (all instances) Within a router, either configure all instances as IP address owners, or no instance as an IP address owner.
  - Assign priority (supervisor) Assign the supervisors different priorities so that the VRRP routers can agree on a master router.
  - Switch on HiVRRP (all instances)
  - Assign to the domain (all instances)
  - Specify sending interval (supervisor)
- Configure HIPER-Ring (in applications as in the above example)
- Define the (Ring) ports as members of the VLANs
- Switch on routing and VRRP globally

Example of configuration of HiVRRP domains

Example of possible settings for the application in figure below.

Subnetwork	IP Address Range	VLAN	VLAN ID
A	10.0.11.0/24	1	11
B	10.0.12.0/24	2	12
C	10.0.13.0/24	3	13
D	10.0.14.0/24	4	14

Table 35: Configuration of the Switches in the subnetwork

Virtual router	VR ID	IP address of the virtual router	Router interface of router A: IP address	Router interface of router B: IP address	VLAN ID
1	11	10.0.11.1/24	10.0.11.2/24	10.0.11.3/24	11
2	12	10.0.12.1/24	10.0.12.2/24	10.0.12.3/24	12
3	13	10.0.13.1/24	10.0.13.2/24	10.0.13.3/24	13
4	14	10.0.14.1/24	10.0.14.2/24	10.0.14.3/24	14

Table 36: Configuration of the two routers

```
enable                          Switch to the Privileged EXEC mode.
vlan database                   Switch to VLAN mode.
vlan 11                         Create VLAN with VID 11.
vlan name 11 VLAN1              Assign name VLAN1 to VID 11.
```

```
vlan routing 11
```
Create a virtual router interface and activate the router function for this VLAN interface.

```
exit
```
Exit the VLAN database mode.

```
show ip vlan
```
Display the virtual router interface the router has setup.

```
           Logical
VLAN ID    Interface     IP Address       Subnet Mask        MAC Address
-------  -----------  ---------------  ---------------  -----------------
11       9/1          0.0.0.0          0.0.0.0          00:80:63:D7:F3:1F
```

```
show ip interface brief
```
Check the entry for the VLAN interface. The purpose is to check the IP address set for the VLAN and the VLAN interface ID.

```
                                          Netdir   Multi
Interface IP Address      IP Mask         Bcast    CastFwd
--------- --------------- --------------- -------- --------
9/1       0.0.0.0         0.0.0.0         Disable  Disable
```

```
configure
```
Switch to Configuration mode. The purpose is to set the IP address for the VLAN interface.

```
interface 9/1
```
Select the VLAN interface.

```
ip address 10.0.11.2 255.255.255.0
```
Set the IP address for this interface.

```
routing
```
Enable routing on this interface.

Next we setup the VRRP and Virtual Router for the interface.

```
ip vrrp 1
```
Create Virtual Router ID (VRID) for the first virtual router at this port.

```
ip vrrp 1 priority 200
```
Assign the virtual router priority 200.

```
ip vrrp 1 mode
```
Enable the first virtual router at this port.

```
ip vrrp 1 ip 10.0.11.1
```
Assign the IP address to VRID.

```
ip vrrp 1 domain 1 supervisor
```
Assign the HiVRRP domain and he domain role to the interface.

```
ip vrrp 1 timers advertise milliseconds 100
```
Assign the advertising time to the interface.

```
exit
```
Exit the configuration mode.

```
exit
```
Exit the Exec mode.

```
show ip vrrp interface 9/1 1
```
Display the configuration for VLAN 11.

```
Primary IP Address..............................10.0.11.1
VMAC Address....................................00:00:5e:00:01:01
Authentication Type.............................None
Base Priority...................................200
Advertisement Interval (milliseconds)..........100
Pre-empt Mode...................................Enable
Administrative Mode.............................Enable
State...........................................Initialized
Current Priority................................200
Preemption Delay (seconds)......................0
Link Down Notification..........................Disabled
VRRP Domain.....................................1
VRRP Domain Role................................Supervisor
VRRP Domain State...............................Supervisor is down
```

```
Advertisement Address..................... 224.0.0.18
```

FIGURE 197 – Setup HiVRRP for VLAN interface

Next define the interface as part of the HiVRRP as member of the VLAN.

`enable`	**Switch to the Privileged EXEC mode.**
`configure`	**Switch to Configure mode.**
`interface 1/5`	**Switch to configuring interface 1/5.**
`vlan participation include 11`	**Assign VLAN interface to this interface.**
`exit`	**Exit Interface Configuration mode.**
`exit`	**Exit Configuration mode.**
`show vlan 11`	**Display configuration for VLAN 11. Here we want to make sure port 1/5 is assigned to VLAN 11.**

```
VLAN ID           : 11
VLAN Name         : VLAN1
VLAN Type         : Static
VLAN Creation Time: 0 days, 04:13:08 (System Uptime)

Interface   Current   Configured   Tagging
----------  --------  -----------  --------
1/1         Exclude   Autodetect   Untagged
1/2         Exclude   Autodetect   Untagged
1/3         Exclude   Autodetect   Untagged
1/4         Exclude   Autodetect   Untagged
1/5         Include   Include      Untagged
1/6         Exclude   Autodetect   Untagged
1/7         Exclude   Autodetect   Untagged
```

Next we switch on routing and VRRP globally.

`enable`	**Switch to the Privileged EXEC mode.**
`configure`	**Switch to Configure mode.**
`ip routing`	**Enable IP routing.**
`ip vrrp`	**Enable VRRP.**
`exit`	**Exit Configuration mode.**
`show ip vrrp`	**Query the VRRP setting for HiVRRP. Note - validate if the Fast switch over instance is configured.**

```
Admin Mode..................................... Enable
Authentication Failure Trap.................... Disable
New Master Trap................................ Disable
Fast instances configured...................... 1
Router Checksum Errors......................... 0
Router Version Errors.......................... 0
Router VRID Errors............................. 0
```

`show ip vrrp interface 9/1 1`	**Query the VLAN interface for the VRRP settings.**

```
Primary IP Address............................. 10.0.11.1
```

```
VMAC Address.................................. 00:00:5e:00:01:01
Authentication Type........................... None
Base Priority................................. 200
Advertisement Interval (milliseconds)......... 100
Pre-empt Mode................................. Enable
Administrative Mode........................... Enable
State......................................... Master
Current Priority.............................. 200
Preemption Delay (seconds).................... 0
Link Down Notification........................ Disabled
VRRP Domain................................... 1
VRRP Domain Role.............................. Supervisor
VRRP Domain State............................. OK
Advertisement Address......................... 224.0.0.18
```

FIGURE 198 – Setup HiVRRP for physical interface and member of VLAN

Repeat the steps across the devices and VLAN interfaces to complete the HiVRRP setup.

VRRP tracking

By monitoring certain router statuses (e.g. line interruption), VRRP tracking makes it possible to switch to a better router when a link goes down.

If there is a line interruption between Switch S1 and router A, router B takes over the master function for virtual router 10.0.1.254. Router A remains the master for virtual router 10.0.2.254. However, router A no longer has a link to subnetwork 10.0.1.0. The virtual router interfaces are independent of each other.

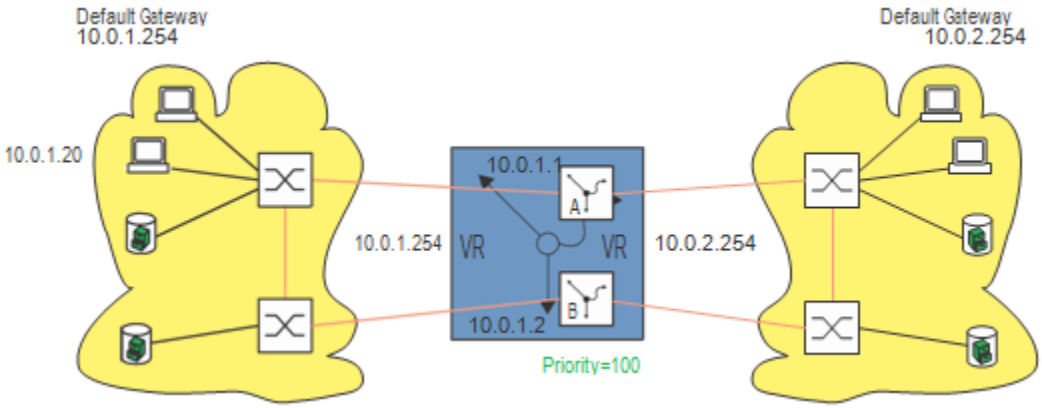


FIGURE 199 – Typical VRRP application

As soon as the VRRP master router with the VRRP tracking function active detects the interruption of one of its links, it lowers its VRRP priority and informs the other VRRP routers of this. Then another VRRP router, which now has the highest priority due to this change in the situation, can take over the master function within the skew time.

Solution without tracking:
Configure router A with a static route to router B or with a dynamic routing procedure, so that router A finds a route into subnetwork 10.0.1.0.

A direct link with preference 0 is the best route. The static route with preference 1 is the second-best route. Then comes the dynamic route.

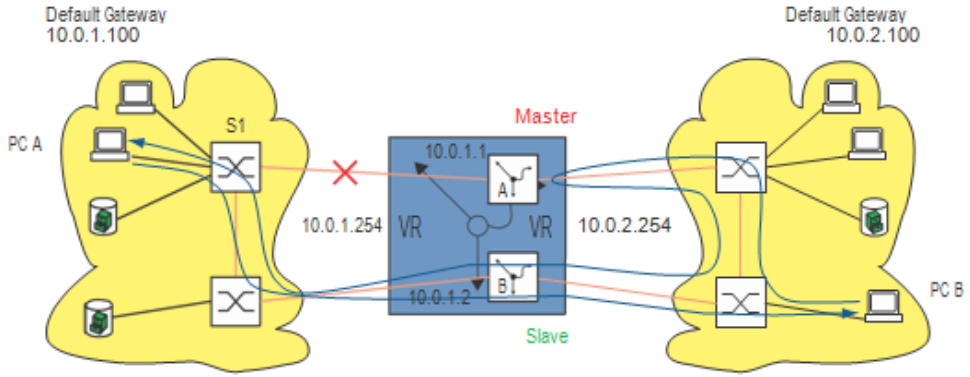


FIGURE 200 – Transmission path from PC B to PC A in the case of a line interruption without tracking

The data from PC B is then transferred to PC A via router A and router B.

Solution with tracking: For an optimal route, the tracking function can now be used to also make router B the master for virtual router 10.0.2.254. By "tracking" the interrupted link and registering the virtual routers for this tracking object, router A decrements its VRRP
priority. Thus when router B receives the next advertisement from router A, router B detects that its own VRRP priority is higher than that of router A and takes over the master function..

Note: As the IP address owner has the fixed VRRP priority 255 by definition, the VRRP tracking function requires the IP addresses of the VRRP router interfaces to differ from the virtual router IP address.

Note: For the backup router to be able to take over the master function from the master router with the lower priority, the VRRP tracking function requires that the preempt mode is activated.

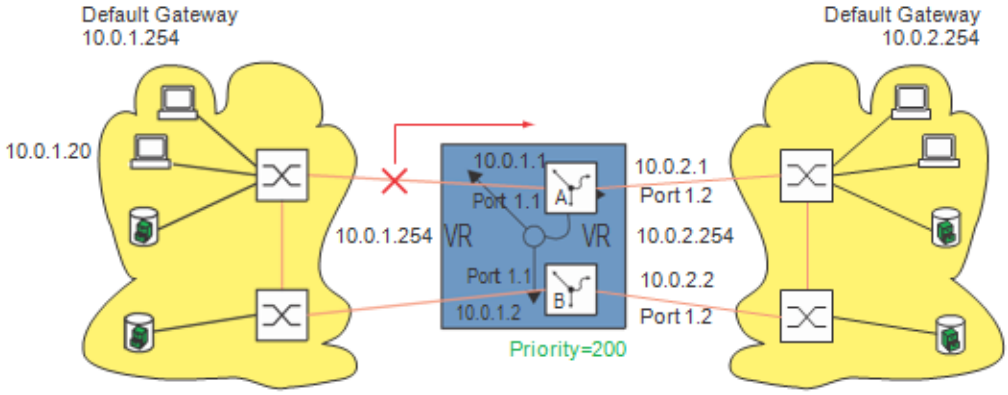


FIGURE 201 – VRRP tracking after a line interruption

	Router A	Router A	Router B	Router B
Interface	1.1	1.2	1.2	1.1
IP address	10.0.1.1/24	10.0.2.1/24	10.0.2.2/24	10.0.1.2/24
VRID	1	2	2	1
VRRP IP address	10.0.1.254	10.0.2.254	10.0.2.254	10.0.1.254
VRRP priority	250	250	200	200
VRRP preemption	Enabled	Enabled	Enabled	Enabled
Track ID	2	1	-	-
Track decrement	100	100	-	-

Table 37: VRRP tracking configuration for the example above

	Router A	Router A	Router B	Router B
Track ID	1	2	-	-
Type	Interface	Interface	-	-
Interface	1.1	1.2	-	-

Table 38: Tracking configuration for the example above

The configuration of VRRP tracking requires the following steps:

- Configure the tracking object
- Configure the VRRP.
- Add the track ID to the VRRP entry (= register the VRRP entry for the tracking object).

In this setup example, we set up interface tracking at port 1.5 with a link down delay of 0 seconds and a link up delay of 3 seconds.

Set up port tracking at port 1.5. In the `Routing:Tracking:Configuration` dialog, click on “Wizard” at the bottom right.

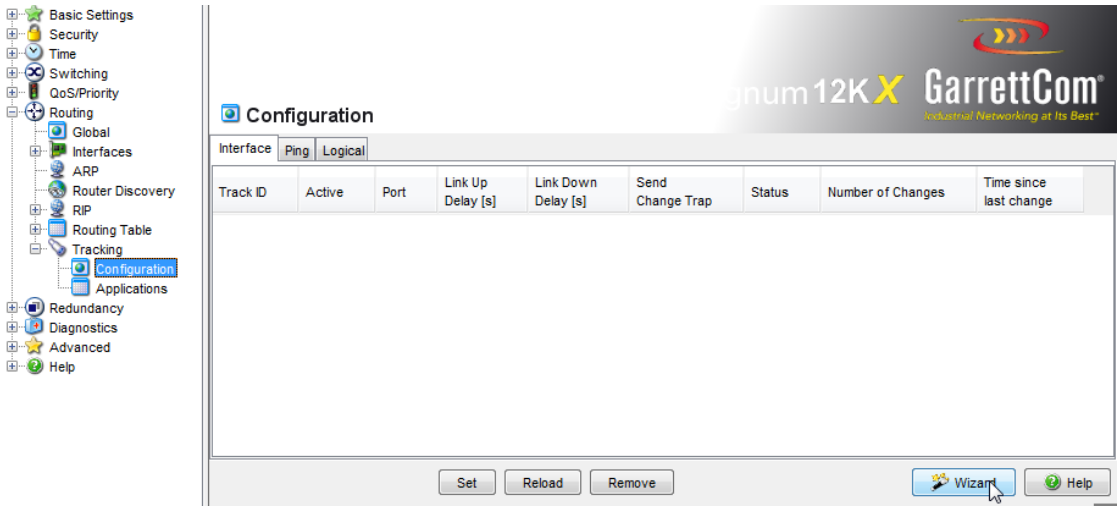


FIGURE 202 – Adding Ping Tracking via the Wizard. Make sure to click on the Logical tab.

Enter the values in the Wizard.

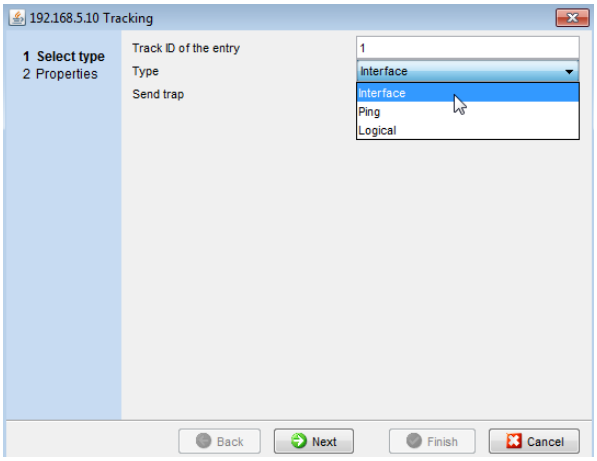


FIGURE 203 – Enter values in the Wizard. Select the type as "Logical".

Enter the values for the Properties as step 2 of the Wizard and click on Finish when done.

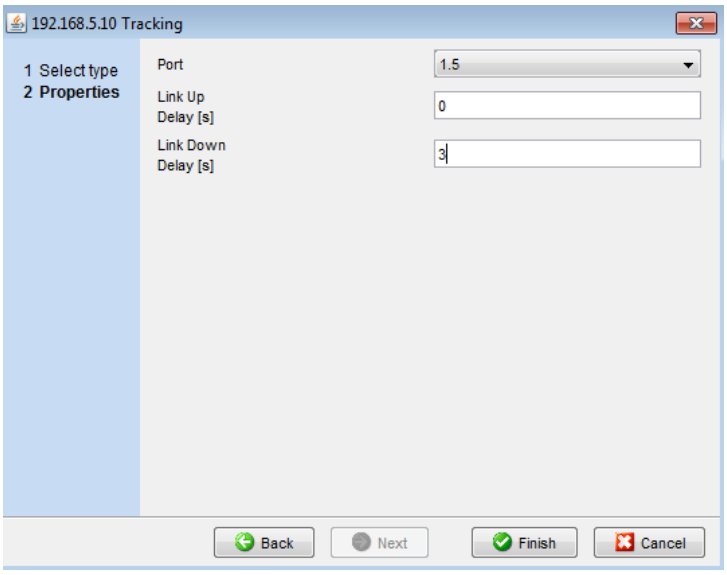


FIGURE 204 – Enter the values for the Properties as shown and click "Finish" when done.

When completed, the entry shows up on the Interface tab.

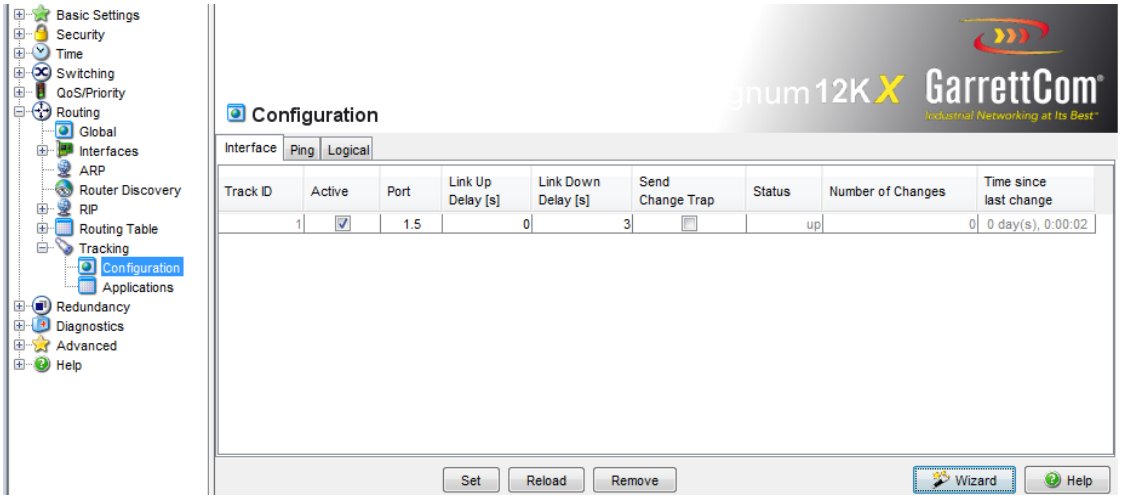


FIGURE 205 – Successful entry for tracking.

```
enable                          Switch to the Privileged EXEC mode.
configure                       Switch to Configuration mode.
track 1 interface 1/5           Enter the tracking information. Note - if the tracking ID
link-down-delay 0               already exists, it is overwritten.
link-up-delay 3

Tracking ID 1 already exists.
  Temporarily disabled for modification.
  Target interface set to 1/5
  Link Down Delay for target interface set to 0 sec
```

```
  Link Up Delay for target interface set to 3 sec
Tracking ID 1 activated
```

FIGURE 206 – Successful entry for tracking using CLI.

Switch on routing and VRRP globally. Note - this step may not be needed as part of the VRRP setup the Routing and VRRP functions had to be enabled. This step is explained earlier and is done using the `Routing:Global` and `Redundancy:VRRP/HiVRRP:Configuration` dialog.

Again in this example, we configure the IP address and VRRP at port 1.5.

Set up port tracking at port 1.5. In the `Redundancy:VRRP/HiVRRP:Configuration` dialog, click on “Wizard” at the bottom right.

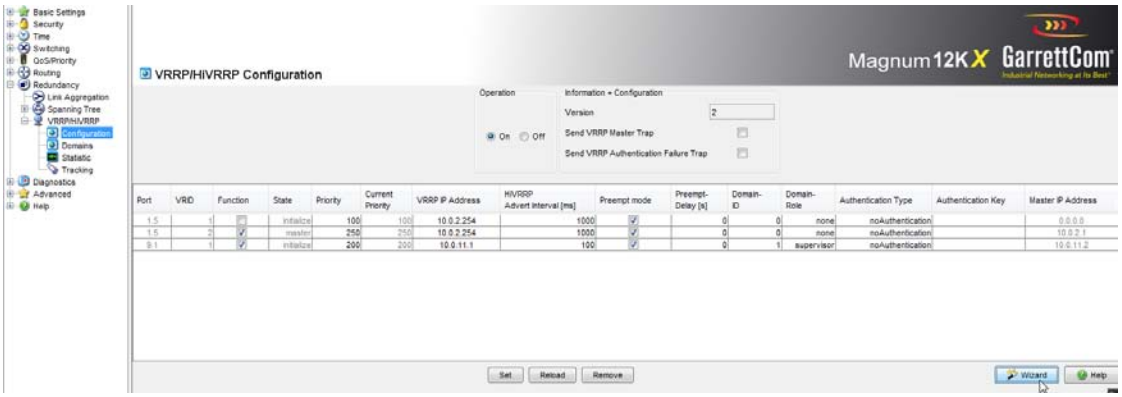


FIGURE 207 – Adding VRRP and tracking.

Enter the values in the Wizard.

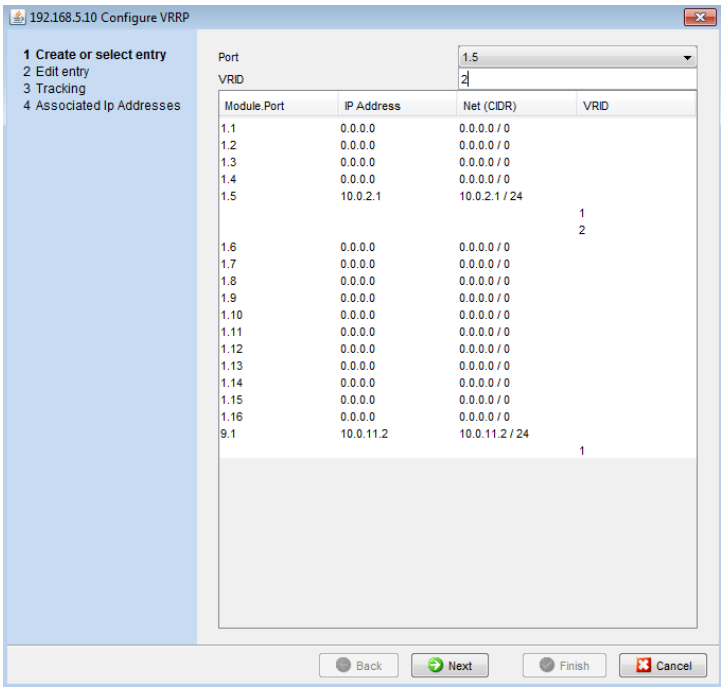


FIGURE 208 – Enter values in the Wizard. Select Port 5 and VRID as 2.

Enter the values for VRRP entry as shown below. Make sure the Preempt mode is checked.

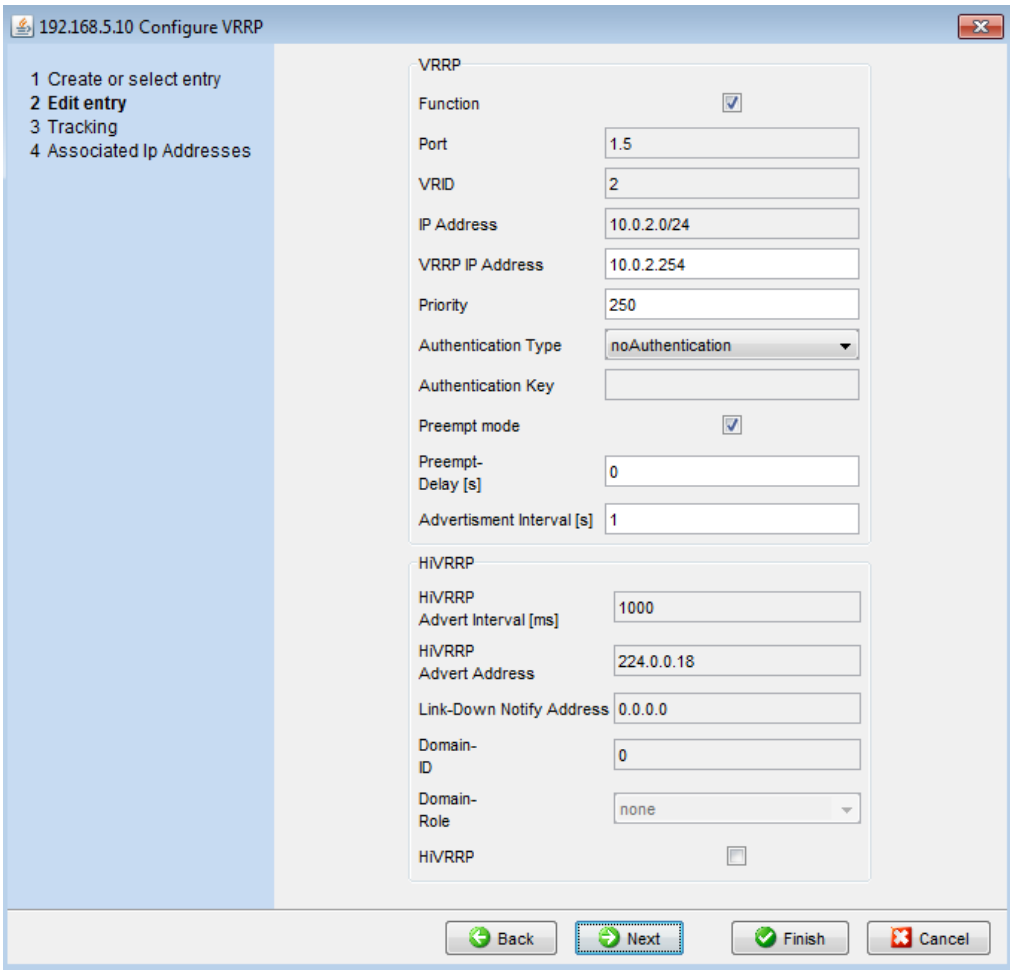


FIGURE 209 – Enter the values for the VRRP entries and click "Next" when done.

Add the tracking ID. Add tracking ID of 2 with a decrement of 100. Click on Add and make sure the entry is added to the window on the right.

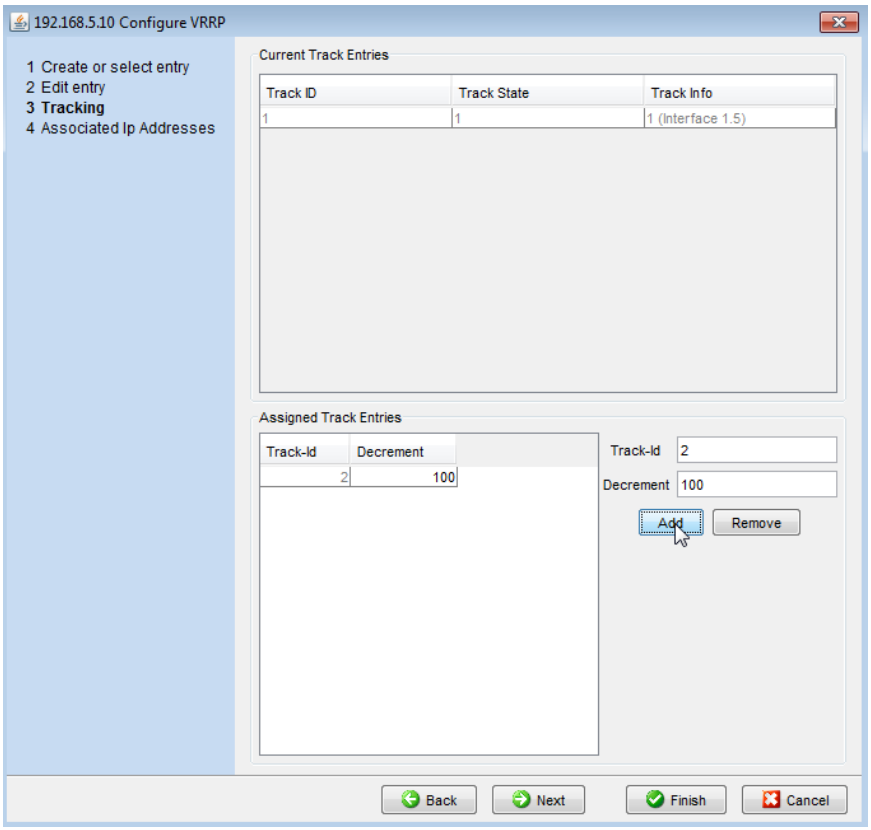


FIGURE 210 – After entering the tracking ID, click "Finish".

When completed, the entry shows up on the Interface tab.

Repeat the same for the other Magnum 12KX switch.

`enable`	**Switch to the Privileged EXEC mode.**
`configure`	**Switch to Configure mode.**
`interface 1/5`	**Switch to configuring interface 1/5.**
`ip address 10.0.2.1 255.255.255.0`	**Assign the IP address.**
`routing`	**Enable routing.**
`ip vrrp 2`	**Create the VRID for the first virtual router at this port.**
`ip vrrp 2 mode`	**Enable the first Virtual router on this port.**
`ip vrrp 2 ip 10.0.2.254`	**Assign the virtual router its IP address.**
`ip vrrp 2 priority 250`	**Assign the virtual router the priority of 250.**

Register the VRRP for tracking

`ip vrrp 2 track 1 decrement`	**Register the VRRP entry for tracking.**

```
100
exit                          Exit out of Interface configuration mode.
exit                          Exit from configuration mode.
show track applications       Display the registered applications.



 TrackId    Application                          Changes     Time since last change
---------  ---------------------------------  ----------  ------------------------
     1      VRRP 1/5 VRID: 2                           0    0 day(s), 03:21:08
```

FIGURE 211 – Configuring VRRP and tracking using CLI.

Repeat the same configuration for the redundant router (second Magnum 12KX switch.)

VRRP with load sharing

With the simple configuration, a router performs the gateway function for all terminal devices. The capacity of the redundant router lies idle. VRRP allows the user to also use the capacity of the redundant router. By setting up a number of virtual routers, different default gateways can be entered on the connected terminal devices and thus steer the data flow. When both routers are active, the data flows via the router on which the IP address of the default gateway has the higher VRRP priority. If a router fails, then all the data flows via the remaining routers.

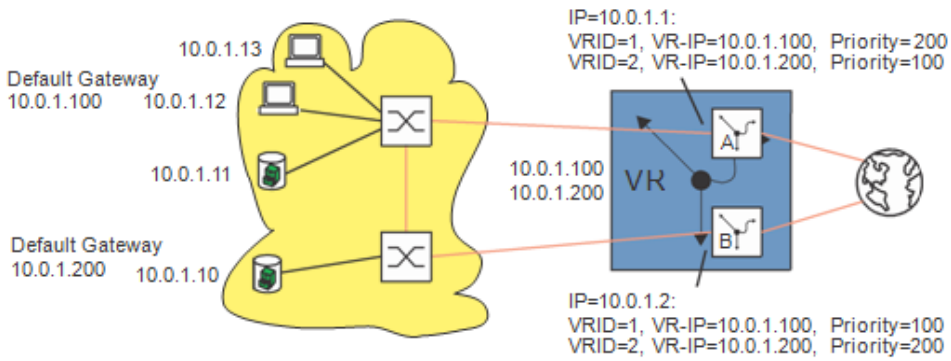


FIGURE 212 – Virtual router with load sharing

To use load sharing, perform the following configuration steps:

- Define a second VRID for the same router interface.
- Assign the router interface its own IP address for the second VRID.
- Assign the second virtual router a lower priority than the first virtual router.
- When configuring the redundant router, make sure to assign the second virtual router a higher priority than the first.
- Give the terminal devices one of the virtual router IP addresses as a default gateway.

VRRP with Multinetting

The router allows the user to combine VRRP with Multinetting.

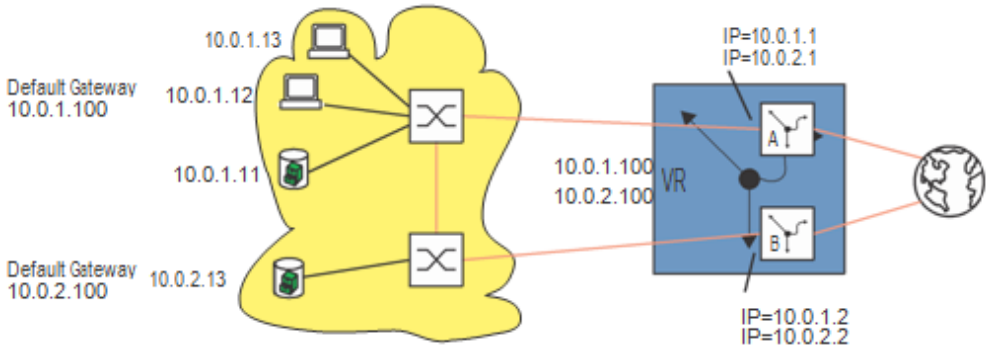


FIGURE 213 – Virtual router with multinetting

To use VRRP with multinetting, perform the following configuration steps on the basis of an existing VRRP configuration.

- Assign a second (secondary) IP address to the port.
- Assign a second (secondary) IP address to the virtual router.

`enable`	**Switch to the Privileged EXEC mode.**
`configure`	**Switch to Configure mode.**
`interface 1/5`	**Switch to configuring interface 1/5.**
`ip address 10.0.2.1 255.255.255.0 secondary`	**Assign the IP address.**
`ip vrrp 1 ip 10.0.2.100 secondary`	**Assign the second IP address to the virtual router with the VRID 1**

FIGURE 214 – Virtual router with multinetting

Perform the same configuration on the redundant router also.

Chapter 20

RIP

The Routing Information Protocol (RIP) is a routing protocol based on the distance vector algorithm. It is used for the dynamic creation of the routing table for routers.

When a router is started, the router only knows the networks directly connected to it, and it sends this routing table to the neighboring routers. At the same time, it requests the routing tables of its neighboring routers. The router adds this information to its routing table and thus learns which networks can be accessed via which routers, and how much effort is involved in this. In order to detect changes in the network (when a router fails or starts), the routers regularly repeat the exchange of all the routing tables, usually every 30 seconds. This involves a considerable bandwidth requirement in large networks.

The costs, also known as the metric, refer to the work involved in reaching a particular network. RIP uses the hop count for this, which describes the number of routers that are traversed along the path to the destination network. The name 'distance vector' is derived from the fact that the distance (metric) is the criterion for determining the route, and the direction is specified by the next hop (vector). The next hop refers to the neighboring router along the path to the destination address.

An entry in the routing table consists of the address of the next hop, the destination address and the metric. The RIP routing table always contains the most efficient route to the destination. This is the route with the smallest metric and the longest suitable network mask prefix.

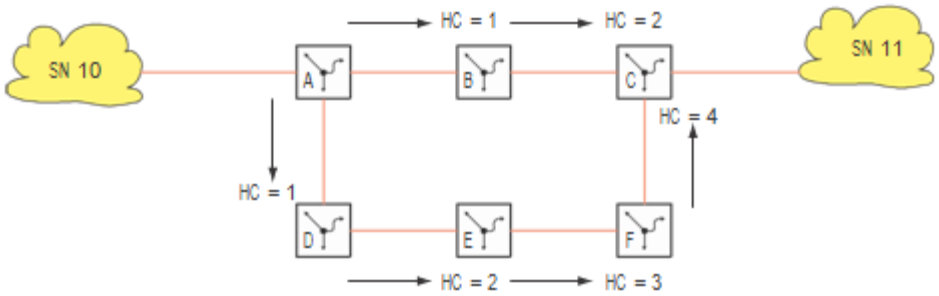


FIGURE 215 – Counting Hops

Router A			**Router B**			**Router D**		
Destination	Next Hop	Metric	Destination	Next Hop	Metric	Destination	Next Hop	Metric
SN 10	lokal	0	SN 10	Router A	1	SN 10	Router A	1
SN 11	Router B	2	SN 11	Router C	1	SN 11	Router E	3

Table 39: Routing table to the figure above

In contrast to OSPF, a RIP router regularly exchanges the content of its entire routing table with its direct neighbor. Every router knows only its own routes and the routes of its direct neighbor. Thus it only has a local perspective.

When changes are made in the network, it takes a while until all the routers have the same uniform view of the network. The process of achieving this condition is known as convergence.

Convergence

How does RIP react to changes in the topography? In the following example of a line interruption between router B and router C, the resulting changes can be seen in the address table:

Assumptions:

- The interruption occurs 5 seconds after B sent its routing table.
- The routers send their routing table every 30 seconds (= default setting).
- There is an interval of 15 seconds between when router A sends its routing table and when router B sends its routing table.

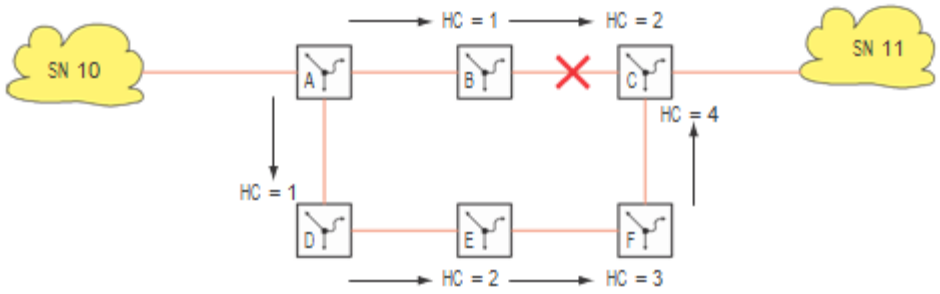


FIGURE 216 – Hop Count

Time elapsing before convergence:

0 seconds: Interruption

10 seconds
Router A sends its routing table:

Router A		
Destination	Next hop	Metric
SN 10	local	0
SN 11	Router B	2

Table 40: Routing table for A

Using the routing table from router A, router B sees that router A knows a connection to destination SN 11 with a metric of 2. Because it does not have its own connection to router C as the next hop to SN 11, router B changes its entry to destination SN 11. It enters router A as the next hop and increases the metric from router A by 1 to 3 (distance = learned distance + 1).

25 seconds Router B sends its routing table:

Router B		
Destination	Next hop	Metric
SN 10	Router A	1
SN 11	Router B	3

Table 41: Routing table for B

Using the routing table from router B, router A sees that router B knows a connection to SN 11 with a metric of 3. So router A increases its metric for SN 11 by 1 to 4.

40 seconds Router A sends its routing table:

Router A		
Destination	Next hop	Metric
SN 10	local	1
SN 11	Router B	4

Table 42: Routing table for C

Using the routing table from router A, router B sees that router A knows a connection to destination SN 11 with a metric of 4. So router B increases its metric for SN 11 by 1 to 5.

55 seconds Router B sends its routing table

Router B		
Destination	Next hop	Metric
SN 10	Router A	1
SN 11	Router A	5

Table 43: Routing table for B

Using the routing table from router B, router A sees that router B knows a connection to SN 11 with a metric of 5. So router A increases its metric for SN 11 by 1 to 6. Because router A can see in the routing table from router D that router D has a connection to SN 11 with the smaller metric of 3, router A changes its entry for SN 11.

70 seconds Router A sends its routing table:

Router A		
Destination	Next hop	Metric
SN 10	Router A	1
SN 11	Router D	4

Table 44: Routing table for A

After 70 seconds, convergence has been achieved again.

Maximum Network Size

The biggest problem with RIP is that routers only know their neighbors directly. This results in long convergence times and the count-to-infinity problem. Infinity refers to the inaccessibility of a destination, and it is designated by hop count 16 in RIP. If the above example did not contain the parallel path via routers D, E and F, then routers A and B would keep sending their routing tables until the metric reached a value of 16. Then the routers recognize that the destination is inaccessible. Using the “split horizon” approach eliminates this looping problem between two neighboring routers. Split horizon has two operating modes.

Simple split horizon	Omits the entries known by a neighbor when sending the routing table to this neighbor
Simple split horizon with poison reverse	Sends the routing table to a neighbor with the entries known by this neighbor, but denotes these entries with the infinity metric (=16).

Thus the hop count 16 specifies the maximum size of a network with RIP as the routing procedure. The longest paths may use up to 15 routers.

General Properties of RIP

The RFC-1058 from June 1988 specifies RIP version 1. Version 1 has the following restrictions: The advantage of RIP is the simple configuration. After the router interface is defined and the RIP is switched on, RIP automatically enters the required routes in the routing table.

- Use of broadcasts for protocol messages.
- Does not support subnetworks/CIDR.
- No authentication.

The standardization of RIP version 2 in the RFC-2453 in 1998 eliminates the above restrictions. RIP V2 sends its protocol messages as a multicast with the destination address 224.0.0.9, and supports subnetwork masks and authentication. However, the restrictions relating to the size of the network remain.

Advantages	Disadvantages
Easy to implement	Routing tables in large networks are very comprehensive
Easy to administrate	Routing information is distributed slowly, because there are fixed sending intervals. This applies in particular to connections that have elapsed, since the routing table only contains existing paths. Can extend to infinity

Table 45: Advantages and disadvantages of Vector Distance Routing

Configuring RIP

The advantage of RIP is the simple configuration. After the router interface is defined and the RIP is switched on, RIP automatically enters the required routes in the routing table.

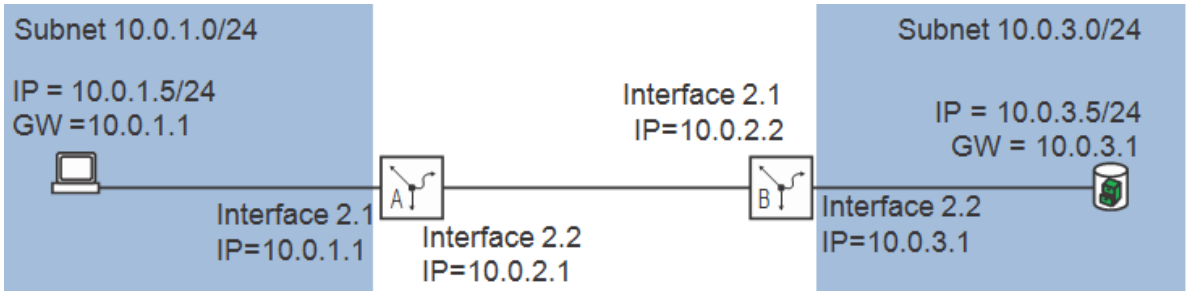


FIGURE 217 – Example of the configuration of RIP

The configuration of RIP requires the following steps:

- Configure router interfaces assign IP address and network mask.
- Switch on RIP on port.
- Switch on RIP globally.
- Switch on routing globally (if this has not already been done).

Set up port tracking at port 1/7. In the `Routing:Interface:Configuration` dialog. Set teh IP address and Mask for port 7 as shown. Enable routing.

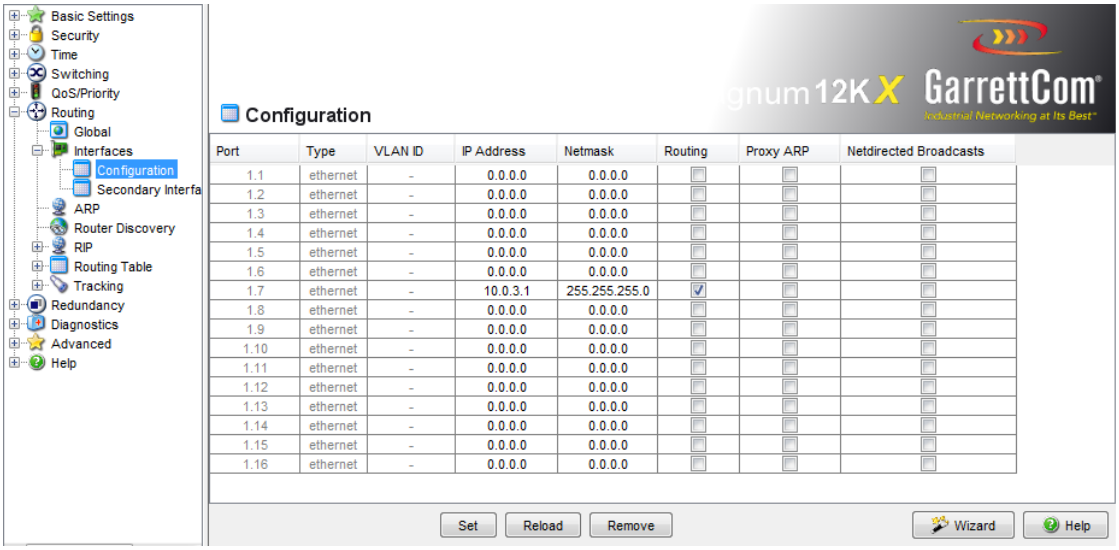


FIGURE 218 – Configure interface with IP address and enable routing on the interface.

Next configure RIP parameters and enable admin on port 1/7 as shown below.

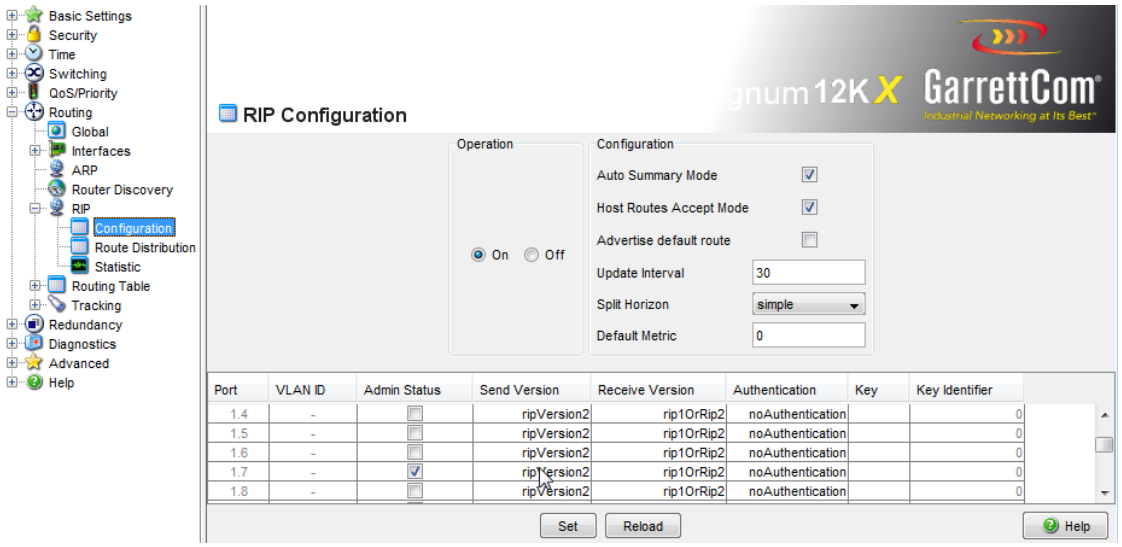


FIGURE 219 – Setup RIP parameters.

Next select Mode so that RIP can distribute routes to other locations as shown below.

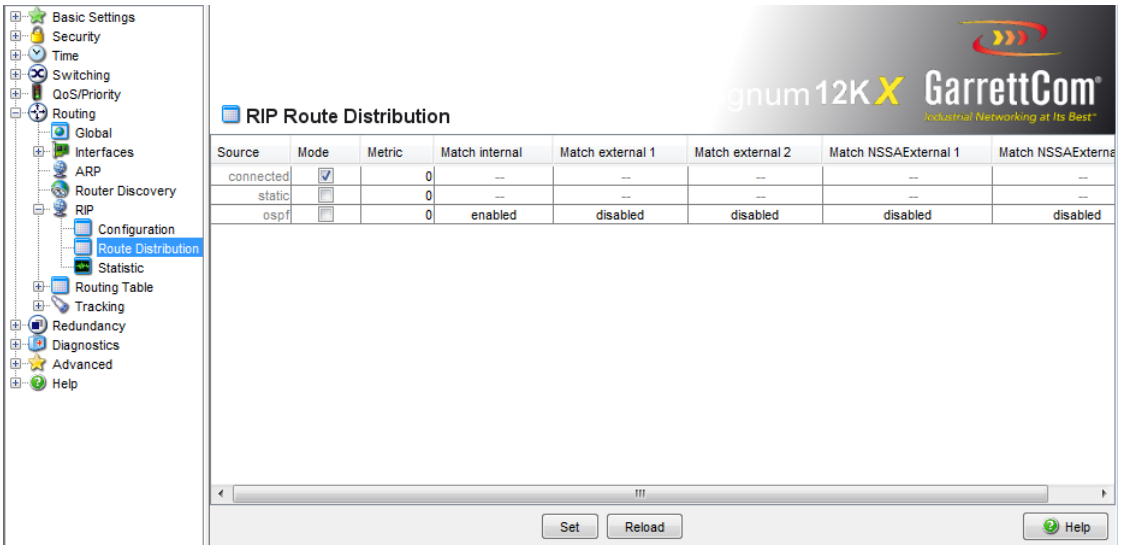


FIGURE 220 – Enable RIP to redistribute routes as shown.

Add any static routes as needed under the `Routing:Routing Table:Static` menu.

Repeat the same for the other Magnum 12KX switch for setting up the RIP protocol.

Configuration for Router B. In the CLI example, we will configure port 1/7 instead of 2.2 as shown above.

`enable` **Switch to the Privileged EXEC mode.**

`configure`	**Switch to Configure mode.**
`interface 1/7`	**Switch to configuring interface 1/7.**
`ip address 10.0.3.1 255.255.255.0 secondary`	**Assign the IP address.**
`routing`	**Enable routing on the interface.**
`ip rip`	**Enable RIP on the port.**
`exit`	**Exit interface configuration mode.**
`exit`	**Exit configuration mode.**
`show ip rip interface brief`	**Display the RIP settings.**

```
                          Send        Receive       RIP         Link
Interface  IP Address     Version     Version      Mode        State
---------  -------------  ----------  ----------  ---------  ----------
1/7        0.0.0.0        RIP-2       both         Enable     Down
```

The IP address entries remain at 0.0.0.0 as long as the routing function is switched off globally.

FIGURE 221 – Configuring RIP on interface as shown above.

For the other router, configure as shown below

`interface 2/1`	**Switch to configuring interface 2/1.**
`ip address 10.0.2.2 255.255.255.0`	**Assign the IP address.**
`routing`	**Enable routing on the interface.**
`ip rip`	**Enable RIP on the port.**
`exit`	**Exit configuration mode.**

FIGURE 222 – Configuring RIP on interface as shown above.

Next we enable routing globally on the Magnum 12KX and instruct RIP to distribute routes.

`enable`	**Switch to the Privileged EXEC mode.**
`configure`	**Switch to Configure mode.**
`router rip`	**Enter the router configuration mode.**
`redistribute connected`	**Instruct RIP to send the routes of the locally connected interfaces along with the learned routes in the RIP information.**
`enable`	**Enable RIP routing.**
`exit`	**Exit the Router Configuration.**
`ip routing`	**Enable Routing for the whole device.**
`show ip rip interface brief`	**Verify the RIP settings.**

```
                          Send        Receive       RIP         Link
Interface  IP Address     Version     Version      Mode        State
---------  -------------  ----------  ----------  ---------  ----------
1/7        10.0.2.2       RIP-2        both         Enable     Up
```

Note - if the interface is down, the IP address shows as 0.0.0.0 and the Link State

shows as down.

`show ip route` **Display the IP routes.**

```
Total Number of Routes..................... 3

   Network          Subnet                  Next Hop    Next Hop
   Address           Mask         Protocol     Intf     IP Address
--------------- --------------- ------------  ------  ---------------
10.0.1.0        255.255.255.0     RIP          2/1      10.0.2.1
10.0.2.0        255.255.255.0     Local        2/1      10.0.2.2
10.0.3.0        255.255.255.0     Local        1/7      10.0.3.1
```

FIGURE 223 – Configuring RIP using CLI.

Perform the corresponding configuration on the other RIP routers also.

Chapter 21

OSPF

Open Shortest Path First (OSPF) is a dynamic routing protocol based on the Link State Algorithm. This algorithm is based on the link states between the routers involved. The significant metric in OSPF is the “OSPF costs”, which is calculated from the available bit rate of a link.

OSPF was developed by IETF. OSPF is currently specified as OSPFv2 in RFC-2328. Along with many other advantages of OSPF, the fact that it is an open standard has contributed to the wide usage of this protocol. OSPF has replaced the Routing Information Protocol (RIP) as the standard Interior Gateway Protocol (IGP) in large networks.

OSPF has a number of significant advantages to offer:

- Cost-based routing metrics: In contrast to RIP, OSPF provides clear metrics based on the bandwidth of each individual network connection. OSPF provides major flexibility in designing a network, because the user can simply change these costs.
- Routing via multiple paths (equal cost multiple path/ECMP): OSPF is able to support a number of equal paths to a given destination. OSPF thus provides efficient utilization of the network resources (load distribution) and improves the availability (redundancy).
- Hierarchical routing: By logically dividing the network into areas, OSPF shortens the time required to distribute routing information. The messages about changes in a subnetwork remain within the subnetwork, without putting any load on the rest of the network.
- Support of Classless Inter-Domain Routing (CIDR) and Variable Length Subnet Mask (VLSM): This allows the network administrator to assign the IP address resources efficiently.
- Fast tuning time: OSPF supports the fast distribution of messages about route changes. This speeds up the tuning time for updating the network topology.
- Saving network resources / bandwidth optimization: Because OSPF, in contrast to RIP, does not exchange the routing tables at regular, short intervals, no bandwidth is unnecessarily “wasted” between the routers.
- Support of authentication: OSPF supports the authentication of all nodes that send routing information.

Advantages	Disadvantages
Every router calculates its routes independently of the other routers.	Complicated to implement
All the routers have the same basic information	Complex administration due to the large number of options.
Rapid detection of link interruptions and rapid calculation of alternative routes.	
The data volume for router information is relatively small, because information is only sent when it is required, and only the information that applies to the immediate neighbor	

Optimal path selection through evaluation of the link quality

Table 46: Advantages and disadvantages of Link State Routing

OSPF-Topology

OSPF is hierarchically structured in order to limit the scope of the OSPF information to be exchanged in large networks. Divide up the network using what are known as areas.

Autonomous System

An Autonomous System (AS) is a number of routers that are managed by a single administration and use the same Interior Gateway Protocol (IGP). Exterior Gateway Protocols (EGP), on the other hand, are used to connect a number of autonomous systems. OSPF is an Interior Gateway Protocol.

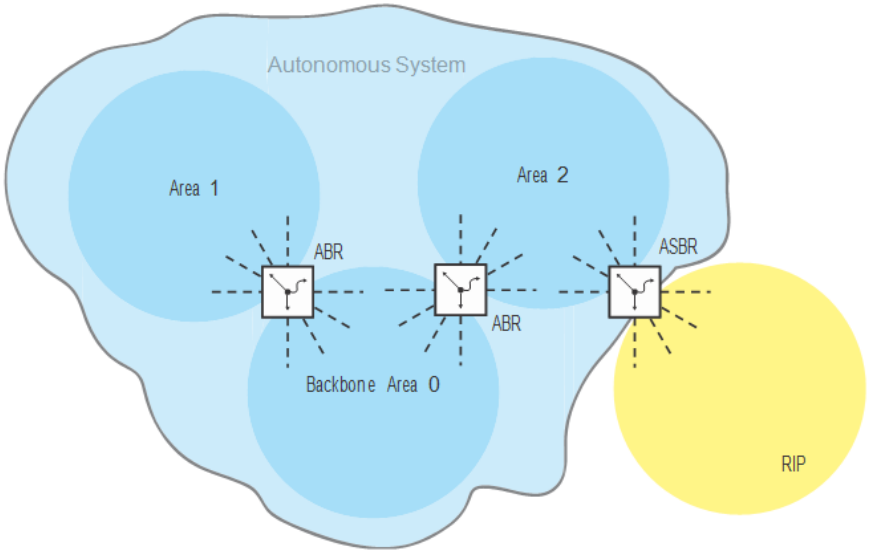


FIGURE 224 – Autonomous System

An AS uses an “Autonomous System Boundary Router” (ASBR) to connect with the outside world. An ASBR understands multiple protocols and serves as a gateway to routers outside the areas. An ASBR is able to transfer routes from different protocols into the OSPF. This process is known as redistribution.

Router ID

The router ID in the form of an IP address is used to uniquely identify every router within an autonomous system. To improve the transparency, it is necessary to manually configure the router ID of every OSPF router. Thus there is no automatic function that selects the router ID from the IP interfaces of the router.

```
enable
```

Switch to the Privileged EXEC mode.

`configure`	**Switch to Configure mode.**
`router ospf`	**Enter the router configuration mode.**
`router-id 192.168.1.0`	**Assign router ID 192.168.1.0.**
`enable`	**Enable OSPF routing.**
`exit`	**Exit OSPF routing setup.**
`exit`	**Exit configuration mode.**

FIGURE 225 – Setup OSPF route ID.

Areas

Each area first forms its own database using the link states within the area. The data exchange required for this remains within the area. Each area uses an Area Border Router (ABR) to link to other areas. The routing information is summarized as much as possible between the areas (route summarization).

Every OSPF router must be a member of at least one area.
An individual router interface can only be assigned to one area. In the state on delivery, every router interface is assigned to the backbone area.

OSPF distinguishes between the following particular area types:

- Backbone-Area:
  This is by definition the area 0 or 0.0.0.0. An OSPF network consists of at least the backbone area. It is the central area, which is linked to all the other areas directly. The backbone area receives all the routing information and is responsible for forwarding this information.

- Stub Area:
  Define an area as a stub area if external LSAs are not to be flooded into the area. External means outside the autonomous system. These external LSAs are the yellow and orange links in the illustration Thus the routers within a stub area only learn internal routes (blue links – e.g. no routes that are exported into OSPF from another log / redistributing). All the destinations outside the autonomous system are assigned to a default route. Stub areas are thus generally used if only one route in the area has a link to outside the area. The use of stub areas keeps the routing table small within the stub area. Totally Stubby Area: Define a totally stubby area if, along with the external (orange and yellow) LSAs, the LSAs of the internal (blue) routes are also not to be sent into the area. Internal means between the areas of the autonomous system. A router within a totally stubby area thus only knows the routes within its own area and the default route out of the area.

  Configuration notes:

  - For a stub area, all the routers within the stub area must be defined as stub routers.
  - A stub area does not allow passage for a virtual link.
  - The backbone area cannot be defined as a stub area.
- Not So Stubby Area (NSSA):
  Define an area as NSSA if the external (yellow) routes of a system directly connected to the NSSA that is outside the autonomous system are to be led into the area (redistributed). These external (yellow) LSAs then also lead from the NSSA to other areas in the autonomous system. External (orange) LSAs within the own autonomous system do not, on the other hand, lead into an NSSA. By using NSSAs, one can integrate ASBRs into the area without foregoing the ad-

vantage of stub areas, namely that external routes from the backbone are not flooded into the corresponding area. Thus NSSAs have the advantage that external routes coming from the backbone are not all entered in the routing tables of the internal routers. At the same time, however, a limited number of external networks (which can be reached across the boundaries of the NSSA) can be propagated into the backbone area.

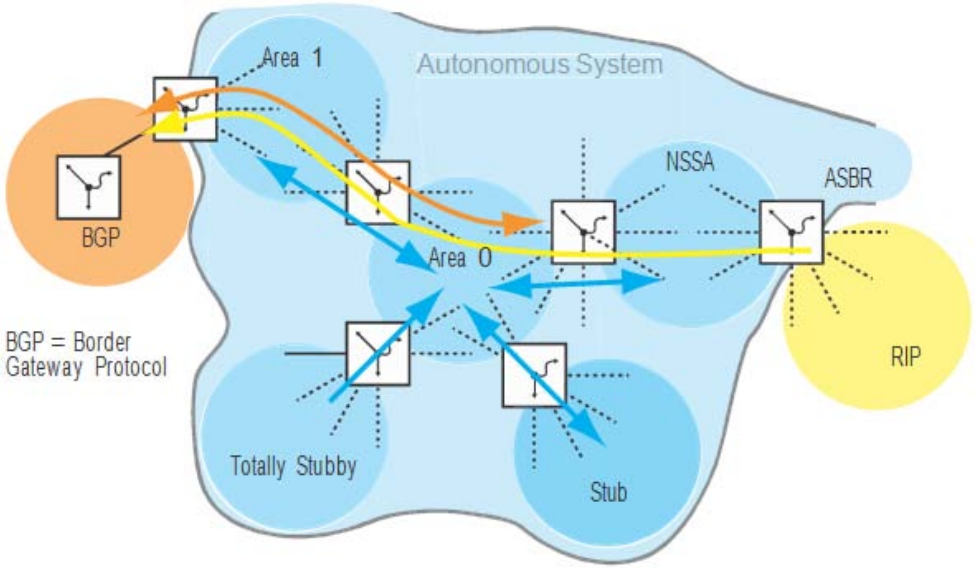


FIGURE 226 – LSA distribution into the area types

`enable`	**Switch to the Privileged EXEC mode.**
`configure`	**Switch to Configure mode.**
`router ospf`	**Enter the router configuration mode.**
`router-id 192.168.1.0`	**Assign router ID 192.168.1.0 for Area 1. Make sure OSPF is disabled. If enabled, use "no enable" command to disable it.**
`router-id 192.168.2.0`	**Assign router ID 192.168.2.0 for Area 2.**
`router-id 192.168.3.0`	**Assign router ID 192.168.3.0 for Area 3.**
`area 192.168.2.0 nssa`	**Define Area 2 as NSSA.**
`area 192.168.3.0 stub`	**Define Area 3 as stub.**
`area 192.168.3.0 default-cost 10`	**Specify the ABR to inject the default route with the metric 10 in the stub area.**
`no area 192.168.3.0 stub summarylsa`	**Configure the Summary LSA mode for the stub area.**

FIGURE 227 – Setup OSPF Areas.

Virtual Link

OSPF requires that the backbone area can be passed through. However, if this is not actually possible, then OSPF provides a virtual link (VL) to connect parts of the backbone area with each other. A VL even allows to connect an area that is connected with the backbone area via another area.

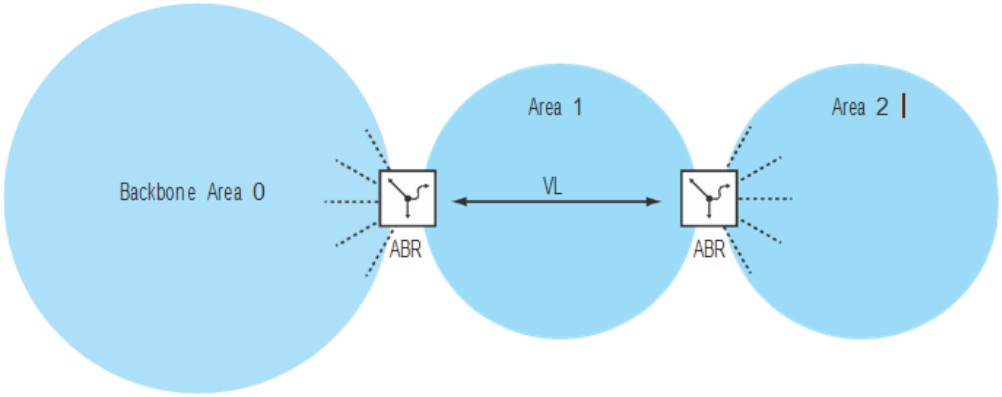


FIGURE 228 – Linking a remote area to the backbone area with a virtual link (VL)

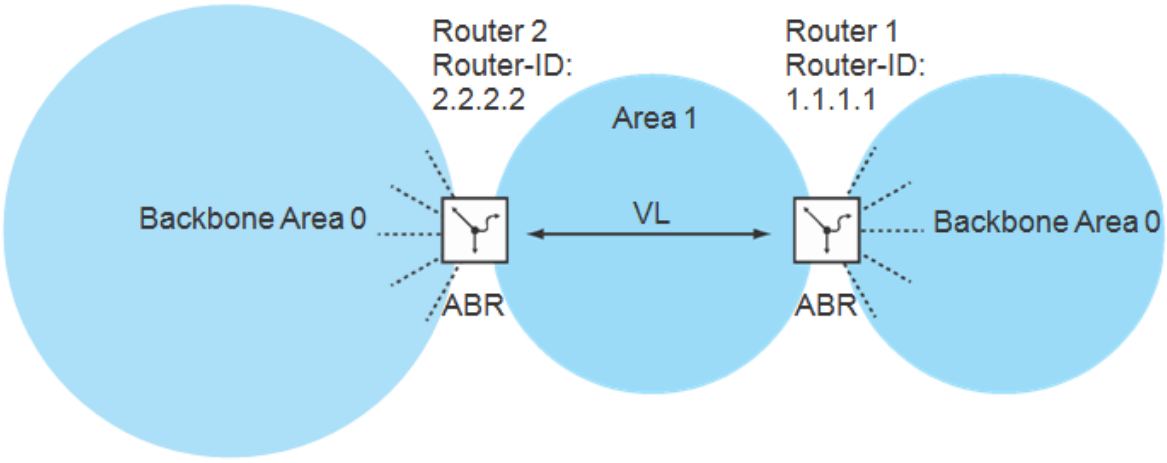


FIGURE 229 – Expanding the backbone area with a virtual link (VL)

Configuration for the expansion of the Backbone area:

Router 1:

`enable`	**Switch to the Privileged EXEC mode.**
`configure`	**Switch to Configure mode.**
`router ospf`	**Enter the router configuration mode.**
`router-id 192.168.1.0`	**Assign router ID 192.168.1.0 for Area 1. Make sure OSPF is disabled. If enabled, use "no enable" command to disable it.**
`router-id 192.168.2.0`	**Assign router ID 192.168.2.0 for Area 2.**
`router-id 192.168.3.0`	**Assign router ID 192.168.3.0 for Area 3.**
`area 192.168.2.0 nssa`	**Define Area 2 as NSSA.**

`area 192.168.3.0 stub`	**Define Area 3 as stub.**
`area 192.168.3.0 default-cost 10`	**Specify the ABR to inject the default route with the metric 10 in the stub area.**
`no area 192.168.3.0 stub summarylsa`	**Configure the Summary LSA mode for the stub area.**
`area 192.168.1.0 virtual-link 2.2.2.2`	**Enter the neighboring router ID for a virtual link to area 1.**

FIGURE 230 – Setup OSPF Areas and Virtual Link.

Configure Router 2 similarly with a virtual link 1.1.1.1.

OSPF Router

OSPF distinguishes between the following router types:

- Internal Router:
  All OSPF interfaces of an internal router are within the same area.
- Area Border Router (ABR):
  ABRs have OSPF interfaces in a number of areas, including the backbone area. ABRs thus participate in multiple areas. Where possible, summarize a number of routes and send “Summary LSAs” to the backbone area.
- Autonomous System Area Border Router (ASBR):
  An ASBR is located on the boundary of an autonomous system and links OSPF to other autonomous systems / routing protocols. These external routes are transferred into OSPF using what is known as redistributing and are then summarized as “AS-external LSAs” and flooded into the area. Switch on the redistributing explicitly. If subnetting use is needed, then enter this explicitly. In OSPF, the following “routing protocols” can be exported:
  - connected (local subnetworks on which OSPF is not switched on),
  - static (static routes),
  - RIP.

Link State Advertisement

As a basis for building up a database via the link states, OSPF uses Link State Advertisements (LSA).

An LSA contains information about

- the router,
- the connected subnets,
- the routes that can be reached,
- the network masks and
- the metrics.

OSPF understands the following LSA-Types:

- Router LSAs (type 1 LSAs):
  Every router sends a router LSA to all its connected areas. They describe the state and the

costs of the router links (router interfaces) that the router has in the corresponding area. Router LSAs are only flooded within the area.

- Network LSAs (Type 2 LSAs):
  These LSAs are generated by the designated router, DR. Setting up the Neighbor Relationship“) and are sent for every connected network/subnet within an area.
- Summary LSAs (type 3 /type 4 LSAs):
  Summary LSAs are generated by ABRs and describe inter-area destinations, meaning destinations in different areas of the same autonomous system.
  Type 3 LSAs describe targets for IP networks (individual routes or summarized routes).
  Type 4 LSAs describe routes to ASBRs.
- AS-external LSAs (type 5 LSAs):
  These LSAs are generated by ASBRs and describe routes outside the autonomous system. These LSAs are flooded everywhere apart from to stub areas and NSSAs.
- NSSA external LSAs (type 7 LSAs):
  A stub area does not flood any external routes (represented by type 5 LSAs) and therefore does not support any Autonomous System Border Routers (ASBRs) at its boundaries. Thus an ASBR cannot carry any routes from other protocols into a stub area. RFC-1587 specifies the functioning of NSSAs. According to RFC-1587, ASBRs send type 7 LSAs instead of type 5 LSAs for the external routes within an NSSA. These type 7 LSAs are then converted into type 5 LSAs by an ABR and flooded into the backbone area. This “translator role” is negotiated among the ABRs in an NSSA (the router with the highest router ID), but it can also be configured manually.

General Operation of OSPF

OSPF was specially tailored to the needs of larger networks and provides a fast convergence and minimum usage of protocol messages.

The concept of OSPF is based on the creation, maintenance and distribution of what is called the link state database. This data basis describes

- all the routers within a routing domain (area) and
- their active interfaces and routes,
- how they are linked to each other and
- the costs of these links.

All the routers within an area have an identical data basis, which means that they all know the exact topology within this area. Every router plays its part in setting up the respective data basis by propagating its local viewpoint as Link State Advertisements (LSAs). These LSAs are then flooded to all the other routers within an area.

OSPF supports a range of different network types such as point-to-point networks (for example, packet over SONET/SDH), broadcast networks (Ethernet) or non-broadcast networks. Broadcast networks are distinguished by the fact that a number of systems (terminal devices, switches, routers) are connected to the same segment and thus can all be addressed simultaneously via broadcasts/multicasts.

OSPF generally performs the following three steps in carrying out its tasks in the network:

- Setting up the neighbor relationships (hello protocol)
- Synchronizing the link state database
- Route calculation

Setting up the Neighbor Relationship

When a router is started, it uses what are called hello packets to contact its neighboring routers. With these hello packets, an OSPF router finds out which OSPF routers are near it and whether they are suitable for setting up a neighbor relationship (adjacency).

In broadcast networks such as Ethernet, the number of neighbors increases with the number of routers connected, as does the information exchange for clarifying and maintaining the neighbor relationships. To reduce these volumes within an area, OSPF uses the hello protocol to determine a Designated Router (DR) within the corresponding segment. Thus every router in an area only sets up the neighbor relationship with its designated router, instead of with every neighbor. The designated router is responsible for the distribution of all the link state information to its neighbor routers. For security reasons, OSPF provides for the selection of a Backup Designated Router (BDR), which takes over the tasks of the DR if the DR fails. The OSPF router with the highest router priority is the DR. The router priority is specified by the administrator. If two routers have the same priority, the router with the higher router ID is selected. The router ID is the smallest IP address of a router interface. Configure this router ID manually when starting up the OSPF router.

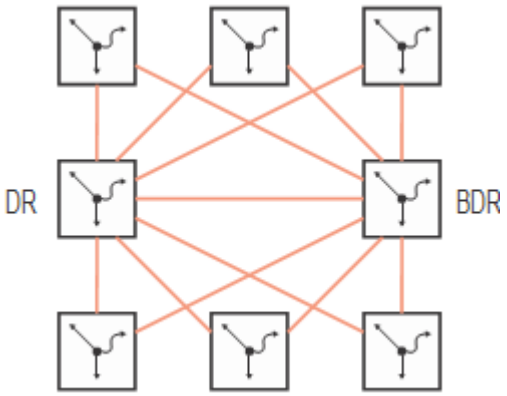


FIGURE 231 – LSA distribution with designated router and backup designated router

To exchange information, OSPF uses reserved multicast addresses.

Destination	Multicast IP address	Mapped multicast MAC address
All OSPF routers	224.0.0.5	01:00:5E:00:00:05
Designated routers	224.0.0.6	01:00:5E:00:00:0

Table 47: OSPF - multicast addresses

Hello packets are also used to check the configuration within an area (area ID, timer values, priorities) and to monitor the neighbor relationships. Hello packets are sent cyclically (hello interval). If hello packets are not received for a specific period (dead interval), the neighbor relationship is terminated and all the corresponding routes are deleted. The hello interval (default: 10 seconds) and the dead interval (default: 30 seconds) can be configured for each router interface, but they must be uniform within an area.

```
enable                    Switch to the Privileged EXEC mode.
configure                 Switch to Configure mode.
```

```
interface 1/10                  Configure interface.
ip ospf hello interval 20       Set hello interval of 20 seconds.
ip ospf dead-interval 60        Set the dead interval of 60 seconds.
exit                            Exit the interface configuration.
exit                            Exit the configuration mode.
show ip ospf neighbor brief     Display the neighbor relationships.
Router ID          IP Address      Neighbor Interface       State
------------       -----------     ------------------       --------
192.168.1.1        10.0.1.1        1/1                      Full
192.168.1.2        11.0.1.1        1/2                      Full
192.168.1.3        12.0.1.1        1/3                      Full
192.168.1.4        13.0.1.1        1/4                      Full
```

FIGURE 232 – Setup OSPF neighbor relationships.

The neighbor relationships can have the following states:

Down	No hello packets received yet.
Init	Receiving hello packets.
2-way	Bidirectional communication, determination of the DR and the BDR.
Exstart	Determination of the master/slave for LSA exchange.
Exchange	LSAs are exchanged or flooded.
Loading	Completion of the LSA exchange
Full	Data basis completely uniform in the area. Routes can now be calculated.

Table 48: OSPF - neighbor states.

Synchronization of the LSD

The central part of the OSPF is the Link State Database (LSD). This database contains a description of the network and the states of all the routers. It is the source for calculating the routing table. It reflects the topology of the network. It is set up after the designated router and backup designated router have been determined within an area (broadcast networks).

To set up the LSD and update any topology changes, the OSPF router sends link status advertisements (LSA) to all the directly accessible OSPF routers. These link status advertisements consist of the interfaces and the neighbors of the sending OSPF router that can be reached via these interfaces. OSPF routers put this information into their databases and flood the information to all the ports.

If no topology changes occur, every router repeats its own LSAs every 30 minutes

The content of the Link State Database can be viewed with the CLI command “show ip ospf database”, whereby the entries are output in accordance with the areas.

```
enable                          Switch to the Privileged EXEC mode.
show ip ospf database           Display the neighbor relationship of the router.
Router Link States (Area 0.0.0.0)

Link Id         Adv Router      Age   Sequence Chksm  Options Rtr Opt
--------------- --------------- ----- -------- ------ ------- -----
192.168.1.1     192.168.1.1     122   80000007 0x5380 -E----  ---E-
192.169.1.1     192.169.1.1     120   80000007 0xbf0e -E----  ---E-

                Network Link States (Area 0.0.0.0)

Link Id         Adv Router      Age   Sequence Chksm  Options Rtr Opt
--------------- --------------- ----- -------- ------ ------- -----
10.0.1.2        192.169.1.1     129   80000002 0xad5a -E----
11.0.1.2        192.169.1.1     135   80000002 0xa066 -E----
12.0.1.2        192.169.1.1     137   80000002 0x9372 -E----
13.0.1.2        192.169.1.1     132   80000002 0x867e -E----

                AS External States

Link Id         Adv Router      Age   Sequence Chksm  Options Rtr Opt
--------------- --------------- ----- -------- ------ ------- -----
192.169.0.0     192.169.1.1     178   80000002 0xca1c
```

FIGURE 233 – Display OSPF neighbor relationships.

The interpretation of the link ID presented depends on the corresponding

Router Link States	Link ID corresponds to router ID of source
Network Link States	Link ID corresponds to interface IP address of the designated router
Network Summary States	Link ID corresponds to the corresponding network
Summary ASBR States	Link ID corresponds to router ID of described ASBR
AS External States	Link ID corresponds to the external network

Route Determination

After the LSDs are learned and the neighbor relationships go to the full state, every router calculates a path to every destination using the Shortest Path First (SPF) algorithm. After the optimal path to every destination has been determined, these routes are entered in the routing table. The route calculation is generally based on the accessibility of a hop and the metric (costs). The costs are added up over all the hops to the destination.

The costs of an individual router interface are based on the available bandwidth of this link. The calculation for the standard setting is based on the following formula:

Metric = 10 000 000 / bandwidth (bits/sec) .

For Ethernet, this leads to the following costs:

10 Mbit	10
100 Mbit	1
1000 Mbit	1 (it is 0.1, rounded up to 1)

Table 49: OSPF - Ethernet interface speed costs.

The table shows that this form of calculation in the standard configuration does not permit any distinction between fast Ethernet and gigabit Ethernet. The standard configuration can be changed by assigning a different value for the costs to each OSPF interface. This enables one to differentiate between fast Ethernet and gigabit Ethernet.

```
enable                  Switch to the Privileged EXEC mode.
configure               Switch to Configure mode.
interface 1/10          Configure interface.
ip ospf cost 2          Assign the cost 2 to interface 1/10.
```

FIGURE 234 – Setup OSPF costs.

Configuring OSPF

Initially, the default values are selected so that one can configure simple OSPF functions in just a few steps. After the router interface is defined and OSPF is switched on, OSPF automatically enters the required routes in the routing table.

The example shows a simple OSPF configuration. Area 0 is already defined configured from the factory. The terminal devices do not have an OSPF function, so the OSPF does not need to be activated on the corresponding router interface. By activating the redistribute function, one can inject the routes to the terminal devices into the OSPF.

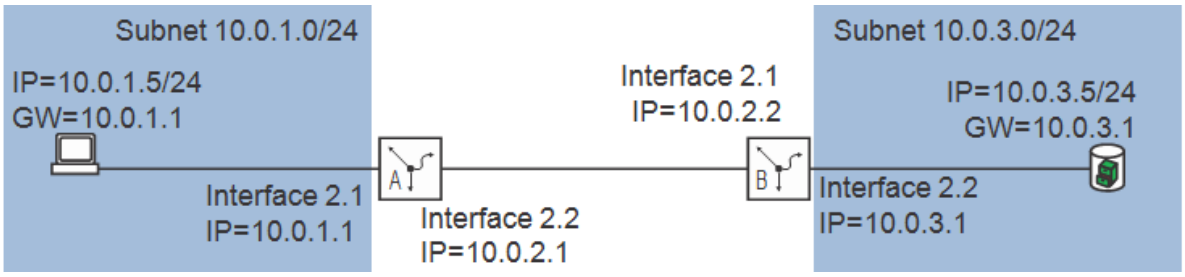


FIGURE 235 – Example of the configuration of OSPF

The configuration of OSPF requires the following steps:

- Configure router interfaces – assign IP address and network mask.
- Switch on OSPF at port.
- Switch on OSPF globally.
- Switch on routing globally (if this has not already been done).

Configuration for Router B

`enable`	**Switch to the Privileged EXEC mode.**
`configure`	**Switch to Configure mode.**
`interface 2/2`	**Configure interface.**
`ip address 10.0.3.1 255.255.255.0`	**Assign IP address to the port.**
`routing`	**Enable routing on the interface.**
`exit`	**Exit from interface configuration mode.**
`interface 2/1`	**Configure next interface.**
`ip address 10.0.2.2 255.255.255.0`	**Assign the IP address.**
`routing`	**Enable routing on this interface.**
`ip ospf`	**Enable OSPF on this interface.**
`exit`	**Exit from the interface configuration.**
`router ospf`	**Switch to the Router configuration mode.**
`enable`	**Enable OSPF globally on the device.**
`router id 10.0.2.2`	**Assign to Router B the router ID of 10.0.2.2**
`redistribute connected subnets`	**Instruct OSPF to,** **- send the routes of the locally connected interfaces along with the learned routes in the RIP information and** **- include subnets without OSPF in OSPF (CIDR).**
`exit`	**Exit Router configuration mode.**
`exit`	**Exit configuration mode.**
`show ip ospf`	**Display the OSPF settings.**

```
Router ID..................................... 10.0.2.2
OSPF Admin Mode.............................. Enable ASBR
Mode.......................................... Enable RFC
1583 Compatibility............................ Enable ABR
Status........................................ Disable
Exit Overflow Interval........................ 0
External LSA Count............................ 0
External LSA Checksum......................... 0
New LSAs Originated........................... 0
LSAs Received................................. 0
External LSDB Limit........................... No Limit
Default Metric................................ Not configured
Default Route Advertise....................... Disabled
Always........................................ FALSE Met-
ric.....................................
Metric Type................................... External Type 2
Maximum Paths................................. 4
Redistributing.............................
Source........................................ Connected
Metric........................................ Not Configured
Metric Type................................... 2
Tag........................................... 0
```

```
Subnets..................................... Yes
Distribute List............................. Not configured
```

`show ip ospf interface brief` **Verify the OSPF settings for the various interfaces.**

```
                                    Router Hello        Dead   Retrax Retrax
     LSAAck Interface AdminMode Area ID    Priority Intval Intval Intval Delay
     Intval
     --------- --------- ----------- -------- ------ ------ ------ -----
     2/1      Enable        0.0.0.0      1        10        40      5      1
     2/2      Disable       0.0.0.0      1        10        40      5      1
```

Next configure the other routers the same way. After configuration, validate the neighborhood relationships.

`show ip ospf neighbor brief` **Verify the OSPF neighbor relationships.**

```
   Router ID               IP Address         Neighbor Interface            State
   ---------------         -----------        ------------------        ---------
   10.0.2.1                10.0.2.1           2/1                          Full
```

`show ip route` **Verify the routing table.**

```
Total Number of Routes...................... 3

Network      Subnet                    Next Hop   Next Hop
Address      Mask           Protocol   Intf       IP Address
---------    -------------  ----------  ---------  -----------
10.0.1.0     255.255.255.0  OSPF ExtT2  2/1        10.0.2.1
10.0.2.0     255.255.255.0  Local       2/1        10.0.2.2
10.0.3.0     255.255.255.0  Local       2/2        10.0.3.1
```

FIGURE 236 – Configuration of OSPF using CLI.

Chapter 22

Protocol-based VLANs

Along with port-based VLANs based on IEEE 802.1Q, the Switch also supports protocol-based VLANs based on IEEE 802.1v.

With port-based VLANs, the Switch uses the port VLAN ID of the receiving port to determine which VLAN a data packet belongs to if it is received without a VLAN tag.

With protocol-based VLANs, the Switch uses the protocol of the received data packet to determine which VLAN a data packet belongs to if it is received without a VLAN tag. The Switch supports the protocols

- IP,
- ARP,
- IPX.

Data packets from other protocols received without a VLAN tag are assigned to a VLAN by the Switch in accordance with the port VLAN ID.

For the VLAN assignment, the Switch takes into account

- firstly, the VLAN tag,
- then the protocol the data packet belongs to,
- and finally, the port VLAN ID.

Protocol-based VLANs enable the uesr to transfer data packets not relevant to routing across IP subnetwork boundaries. Data packets relevant to routing are IP and ARP data packets.

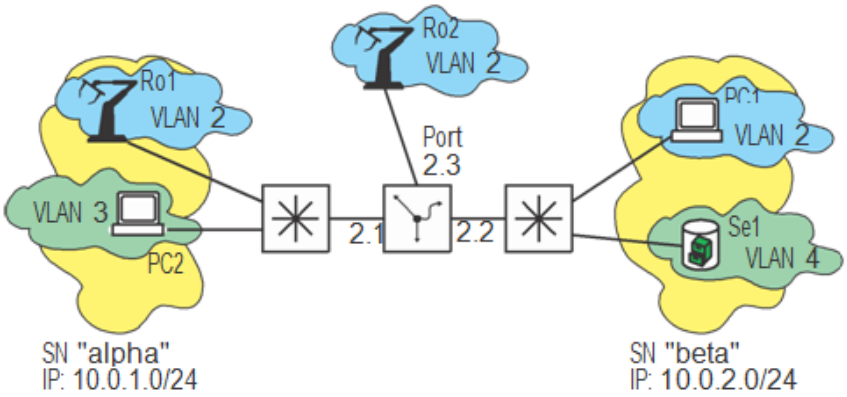


FIGURE 237 – Example of a protocol-based VLAN

In the example PC2 and Se1 communicate via IP. These data packets are routed. The devices Ro1, Ro2 and PC1 communicate via other Ethernet-based protocols. These data packets are switched in VLAN 2. Thus all IP data packets remain in their subnetworks, apart from the IP data packets that are meant for a different subnetwork.

Configuration Example

```
enable                          Switch to the Privileged EXEC mode.
configure                       Switch to Configure mode.
vlan protocol group alpha       Create a VLAN protocol group called alpha.
vlan protocol group beta        Create a VLAN protocol group called beta.
exit                            Exit Configuration mode.
show protocol all               Display the protocol setup configuration.
                  Group
   Group Name       ID    Protocol(s)  VLAN       Interface(s)
---------------  ------  -----------  ----  ------------------------
alpha            1                    0
beta             2                    0
configure                       Switch to Configure mode.
vlan protocol group add         Add the IP protocol for Group ID 1 (Alpha).
protocol 1 ip
vlan protocol group add         Add the ARP protocol for Group ID 1 (Alpha).
protocol 1 arp
vlan protocol group add         Add the IP protocol for Group ID 2 (Beta).
protocol 2 ip
vlan protocol group add         Add the ARP protocol for Group ID 2 (Beta).
protocol 2 arp
exit                            Exit Configuration mode.
show protocol all               Display the protocol setup configuration. Here we want
                                to verify that the Protocols IP and ARP have been
                                added.
                  Group
   Group Name       ID    Protocol(s)  VLAN       Interface(s)
---------------  ------  -----------  ----  ------------------------
alpha            1       IP,ARP       0
beta             2       IP,ARP       0
vlan database                   Configure VLANs.
vlan 2                          Create VLAN 2.
vlan 3                          Create VLAN 3.
vlan 4                          Create VLAN 4.
vlan routing 3                  Create a virtual routing interface for VLAN 3.
vlan routing 4                  Create a virtual routing interface for VLAN 4.
protocol group 1 3              Assign the protocol group 1 with VLAN 3
protocol group 2 4              Assign the protocol group 2 with VLAN 4.
exit                            Exit VLAN setup mode.
show protocol all               Display the protocol setup. Here we want to verify that
                                the protocol groups are associated with the VLANs.
                  Group
   Group Name       ID    Protocol(s)  VLAN       Interface(s)
---------------  ------  -----------  ----  ------------------------
alpha            1       IP,ARP       3
```

```
beta              2       IP,ARP       4
```

`show ip vlan` — **Display the IP interface and IP addresses associated with VLANs.**

```
           Logical
VLAN ID    Interface     IP Address       Subnet Mask        MAC Address
-------  -----------  ---------------  ---------------  -----------------
3        9/1          0.0.0.0          0.0.0.0          00:80:63:D7:F3:1F
4        9/2          0.0.0.0          0.0.0.0          00:80:63:D7:F3:20
```

`configure`	**Switch to Configure mode. Now we configure IP addresses and VLAN assignments to the protocol groups.**
`interface 1/8`	**Select the interface which needs to be configured.**
`vlan participation exclude 1`	**Remove VLAN 1 from this interface.**
`vlan participation include 2`	**Add VLAN 2 to this interface.**
`vlan participation include 3`	**Add VLAN 3 to this interface.**
`vlan pvid 2`	**Assign the default VLAN for this port as VLAN 2. What this does is that the IP and ARP packets from this port are tagged with VID 2.**
`protocol vlan group 1`	**This command assigns the IP and APR packets in this protocol group 1 to its associated VLAN (see "show protocol all" command above). In this situation, the VLAN associated is VLAN 3.**
`exit`	**Exit from interface configuration.**
`show protocol all`	**Note – now we should see interface added to the protocol group 1 (Alpha).**

```
                 Group
   Group Name      ID    Protocol(s)  VLAN       Interface(s)
---------------  ------  -----------  ----  ------------------------
alpha            1       IP,ARP       3     1/8
beta             2       IP,ARP       4
```

`configure`	**Switch to Configure mode. Now we configure IP addresses and VLAN assignments to the second protocol group.**
`interface 1/9`	**Select the interface which needs to be configured.**
`vlan participation exclude 1`	**Remove VLAN 1 from this interface.**
`vlan participation include 2`	**Add VLAN 2 to this interface.**
`vlan participation include 4`	**Add VLAN 3 to this interface.**
`vlan pvid 2`	**Assign the default VLAN for this port as VLAN 2. What this does is that the IP and ARP packets from this port are tagged with VID 2.**
`protocol vlan group 2`	**This command assigns the IP and APR packets in this protocol group 1 to its associated VLAN (see "show protocol all" command above). In this situation, the**

```
                                  VLAN associated is VLAN 4.
exit                              Exit from interface configuration.
show protocol all                 Note – now we should see interface added to the pro-
                                  tocol group 2 (Beta).
                  Group
   Group Name       ID    Protocol(s)  VLAN       Interface(s)
---------------  ------  -----------  ----  ------------------------
alpha            1       IP,ARP       3     1/8
beta             2       IP,ARP       4     1/9
interface 1/10                    Select the interface which needs to be configured.
vlan participation exclude        Remove VLAN 1 from this interface.
1
vlan participation include        Add VLAN 2 to this interface.
2
vlan pvid 2                       Assign the default VLAN for this port as VLAN 2. What
                                  this does is that the IP and ARP packets from this port
                                  are tagged with VID 2.
exit                              Exit from interface configuration.
Next we configure the IP addresses of the VLANs and set up routing between the VLANs.
interface 9/1                     Configure the first VLAN interface.
ip address 10.0.1.1               Set the IP address for this VLAN interface.
255.255.255.0
routing                           Enable routing on this VLAN interface.
exit                              Exit the interface configuration.
interface 9/2                     Configure the first VLAN interface.
ip address 10.0.2.1               Set the IP address for this VLAN interface.
255.255.255.0
routing                           Enable routing on this VLAN interface.
exit                              Exit the interface configuration.
exit                              Exit the configuration interface.
show ip interface brief           Display the IP addresses setup on the interfaces.
                                          Netdir   Multi
Interface IP Address      IP Mask         Bcast    CastFwd
--------- --------------- --------------- -------- --------
9/1       10.0.1.1        255.255.255.0   Disable  Disable
9/2       10.0.2.1        255.255.255.0   Disable  Disable

configure                         Enter the configuration mode.
ip routing                        Enable routing on the switch.
```

FIGURE 238 – Configuring Protocol VLANs using CLI.

Chapter 23

Multicast Routing

Multicast data streams are data packets that a sender sends to multiple recipients. To reduce the network load, the sender uses a Multicast address. The user thus sends each packet only once to the Multicast address instead of sending it to each recipient individually. The recipients recognize a Multicast data stream intended for them by the Multicast address. A common reason for introducing subnetworks is the restriction of broadcast data streams. Switches send broadcast/Multicast data streams to all ports, while routers block broadcast/Multicast data streams. Multicast routing enables the user to accurately transmit Multicast data streams beyond the boundaries of subnetworks. Accurate transmission means sending data streams with defined Multicast addresses exclusively to those devices which want to receive the Multicast data stream.

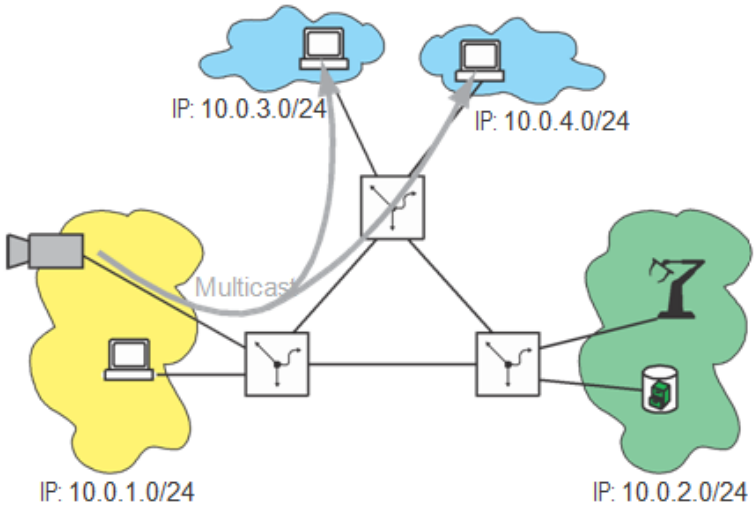


FIGURE 239 – Multicast routing requires

To the use of Multicast routing pertains:

- Defined Multicast addresses
- A protocol for Multicast group registration that organizes the exchange of information by means of Multicast data streams (e.g. IGMP). This information relates to the reporting that network participants wish to receive Multicast data streams and querying this wish by means of intermediate devices.
- A protocol that guides the Multicast data streams in accordance with the information on Multicast data streams (e.g. PIM-DM, DVMRP).

Multicast Addresses

IP Multicast Addresses

The IANA (Internet Assigned Numbers Authority) defines the IP addresses of the class D IP address space as Multicast addresses. IP Multicast addresses are in the range from 224.0.0.0 to 239.255.255.255.

IP address range	Assignment
224.0.0.0	Base address, reserved
224.0.0.1 - 224.0.0.255	Local Network Control Block, reserved for routing protocols, IGMP, etc. For example: 224.0.0.1 - all hosts of a subnetwork 224.0.0.2 - all routers of a subnetwork 224.0.0.4 - all DVMRP routers 224.0.0.5 - all OSPF routers 224.0.0.6 - all OSPF DR routers 224.0.0.9 - all RIP v2 routers 224.0.0.13 - all PIM routers 224.0.0.18 - all VRRP routers 224.0.0.22 - all IGMP v3 reports
224.0.1.0 - 224.0.1.255	Internetwork Control Block
224.0.2.0 - 224.0.255.255	AD HOC Block
224.1.0.0 - 238.255.255.255	Various organizations, protocols, applications, reservations. For example: 232.0.0.0-232.255.255.255 - Source-specific Multicasts
239.0.0.0 - 239.255.255.255	Administratively scoped IP v4 Multicast space These Multicast addresses are not transferred by any router beyond the local boundaries and into the Internet. Therefore the administrator can assign these addresses any way he wants within these local boundaries.

Table 50: Assignment of the IP Multicast address range

The administratively scoped IP v4 Multicast area is subdivided further by the IANA:

IP address range	Assignment
239.000.000.000 - 239.191.255.255	Reserved [IANA]
239.192.000.000 - 239.251.255.255	Organization-local scope [Meyer, RFC2365]
239.252.000.000 - 239.254.255.255	Site-local scope (reserved) [Meyer, RFC2365]
239.255.000.000 - 239.255.255.255	Site-local scope [Meyer, RFC2365]

Table 51: Assignment of the administratively scoped IP v4 Multicast area

In the end, the following multicast IP address ranges are left over for disposal by an organization's administrator:

- 239.192.000.000 - 239.251.255.255 for an organization's local areas.
- 239.255.000.000 - 239.255.255.255 for an organization's entire area.

Note: When selecting the Multicast IP addresses, ensure that they can be uniquely mapped onto MAC Multicast addresses.

MAC Multicast Addresses

The IEEE calls the 48-bit MAC address an “Extended Unique Identifier”. It is the unique identifier of a device. The first 24 bits of the MAC address (Organizationally Unique Identifier, OUI) is assigned by the IEEE to the manufacturer. The manufacturer uses the last 24 bits to uniquely identify their device interfaces.

A number of MAC addresses are reserved for specific applications:

MAC-Address	Type	Use
01-00-5E-00-00-00	0800	Internet Multicast [RFC1112]
01-80-C2-00-00-00	-802-	Spanning tree (for bridges)
FF-FF-FF-FF-FF-FF	0806	ARP (for IP and CHAOS) as needed
FF-FF-FF-FF-FF-FF	8035	Reverse ARP

Table 52: Examples of reserved MAC addresses

Mapping IP MAC Multicast Addresses

When IP data packets are sent via Ethernet, the IP address is assigned to a MAC address, and therefore IP Multicast addresses are also mapped onto MAC Multicast addresses. The 23 lower-value bits of the 32-bit IP Multicast address make up the 23 lower-value bits of the 48-bit MAC Multicast address. Of the remaining 9 bits of the IP Multicast address, 4 bits are used as the class D identification for the Multicast address. The remaining 5 bits ensure that 32 IP Multicast addresses can be mapped onto one and the same MAC Multicast address.

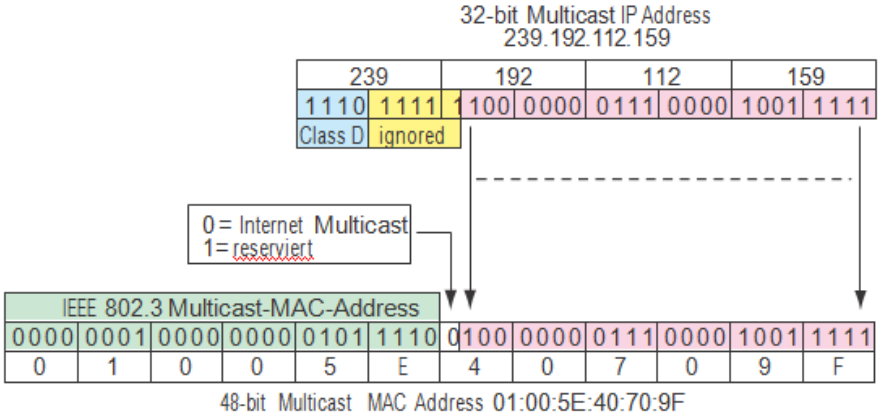


FIGURE 240 – Conversion of the IP address to the MAC address

Multicast Group Registration

The Internet Group Management Protocol (IGMP) describes the distribution of Multicast information between routers and terminal devices on Layer 3. Routers with an active IGMP function periodically send queries to find out which IP Multicast group members are connected to the LAN, or to find out who is interested in becoming a group member. Multicast group members reply with a Report message. This Report message contains all the parameters required by the IGMP. The router records the IP Multicast group address from the Report message in its routing table. The result of this is that it transfers frames with this IP Multicast group address in the target address field only in accordance with the routing table.

Devices which no longer want to be members of a Multicast group can cancel their membership by means of a Leave message (from IGMP version 2), and they do not transmit any more Report messages. The router removes the routing table entry if it does not receive any Report messages within a specified period of time (aging time).

If there are multiple routers with an active IGMP function in the subnetwork, then

- for IGMP version 1, all routers in this subnetwork periodically send queries
- for IGMP versions 2 and 3, the routers decide which router takes over the query function (Querier Election).

Protocol	Standard
IGMP v1	RFC 1112
IGMP v2	RFC 2236
IGMP v3	RFC 3376

Table 53: Standards which describe the Multicast Group Membership Discovery.

An advantage that IGMP version 2 has over IGMP version 1 is that a Multicast recipient can cancel his membership in a Multicast group, thus freeing up his bandwidth more quickly. Another advantage is the introduction of the Querier Election.

IGMP version 3 provides more security with the Source Filtering option. Multicast recipients can define the sources from which they want to receive Multicast data streams. The router blocks Multicast data streams with other source addresses.

The different versions of IGMP are compatible downwards. This means that an IGMP version 3 router can also process version 1 and version 2. If there are different IGMP versions in a subnetwork, the participating routers agree on the smallest version.

PIM-DM/PIM-SM/DVMRP

PIM-DM (Protocol Independent Multicast Dense Mode) is a routing protocol that uses the available Unicast routing table of other protocols to steer Multicast data streams. This ability, and the fast convergence it enables, is the reason why PIM-DM is now very widely-used.

The DVMRP (Distance Vector Multicast Routing Protocol) is a routing protocol that uses its own distance vector algorithm to create its own Multicast routing table. DVMRP works similarly to RIP and is limited to 32 hops. In the past, DVMRP was very widely-used, and today it is used because of its compatibility with existing applications.

Both protocols use what is known as the Implicit Join method, which means that a participant who has left the Multicast data stream is not included in the data flow. To enable a participant who has left to receive Multi case data streams again, the routers transmit to all participants again after the hold time has elapsed. For DVMRP, the hold time is fixed at 2 hours. For PIM-DM, the variable hold time is set at 210 seconds. PIM-DM requires that the user set the hold time to the same value for all the participating routers.

DVMRP	PIM-DM
Knows the topology better because DVMRP uses its own protocol.	Fast convergence Optimization through changeable timers

Table 54: Advantages of the protocols

PIM-SM (Protocol Independent Multicast Sparse Mode) is an extended variant of PIM-DM.
This version of PIM is mainly suitable for networks with a restricted bandwidth (e.g. WANs) and for networks with few participants from Multicast groups.

PIM-SM differs from PIM-DM and DVMRP in the following ways, as regards subscribing and unsubscribing participants:

- PIM-DM and DVMRP assume that very many participants are interested in the Multicast groups. Therefore, at the start of the communication, PIM- DM and DVMRP flood the information about available Multicast groups into the entire network. Participants who are not interested in a Multicast group unsubscribe from this group explicitly.
- In contrast, PIM-SM assumes that very few participants in the network are interested in the Multicast groups. PIM-SM waits for the participants to actively subscribe without itself sending information about available Multicast groups to the network. All participants who are interested in a Multicast group subscribe to a group explicitly. With this procedure, PIM- SM reduces the data traffic in the network.

How PIM-DM and DVMRP function

In the first step for setting up the Multicast routes, a PIM-DM/DVMRP router floods Multicast data streams to all ports, with the exception of the receiving port (= flooding).

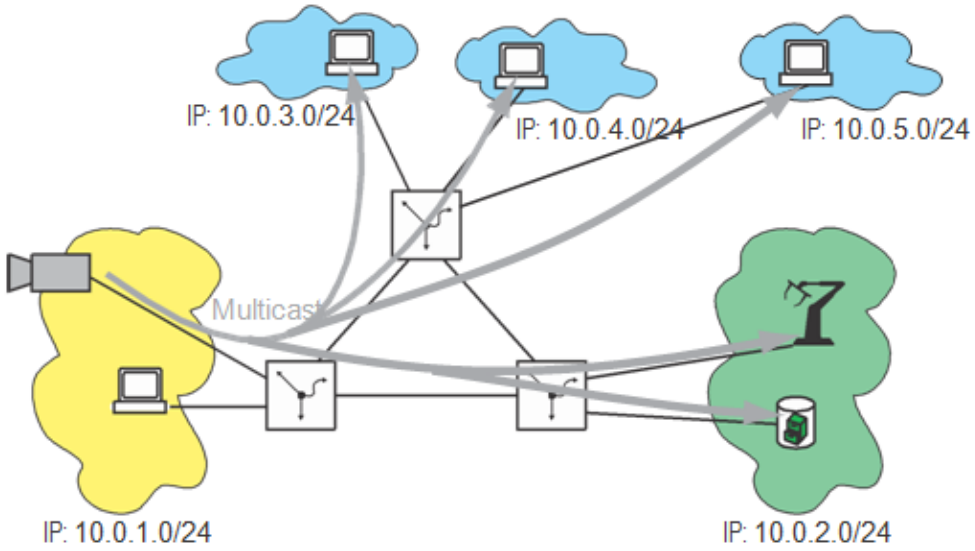


FIGURE 241 – Multicast Flooding

Routers that are not interested in the Multicast data stream send what are known as prune messages so that they will not be sent any Multicast data streams from this source in the future. The routers send the prune messages back in the direction from which they received the Multicast data streams (upstream).

A router transmits a Multicast data stream until the hold time has elapsed,

- When it is using IGMP to determine a Multicast recipient which is connected to a port directly or via a switch or
- When a router that is connected to a Multicast recipient is connected directly to a port.

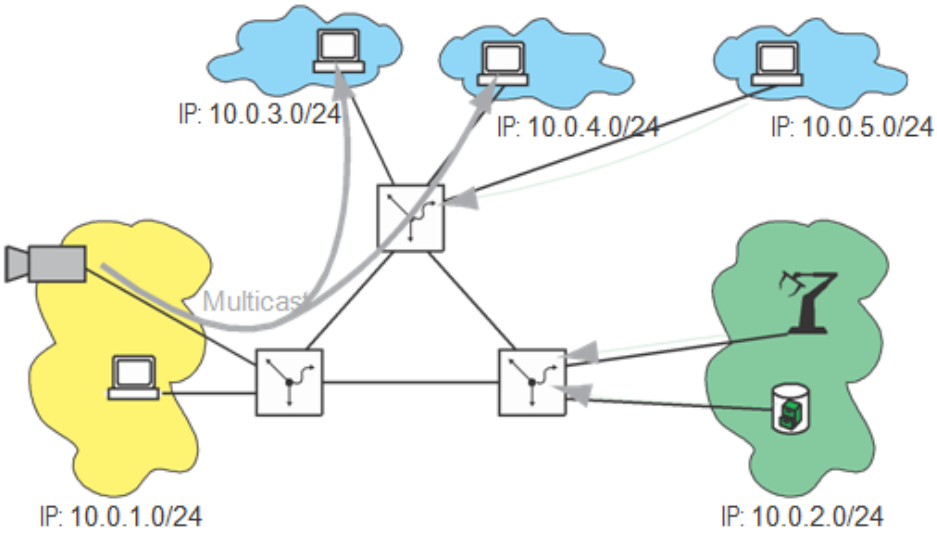


FIGURE 242 – Multicast Pruning

In the second step, PIM-DM/DVMRP calculates the shortest paths (SPT - Shortest Path Tree) between the Multicast source and the Multicast recipients. The result is the source-routed Multicast distribution tree. Source routed means that the calculation method is tracing back from the recipient to the source (RPF - Reverse Path Forwarding). To avoid loops, RPF rejects all Multicast data streams received at a port that do not belong to the shortest path.

The method of the shortest paths is very efficient with regard to the data paths. However, it does have the

disadvantage that, depending on the topology, the routers requires a lot of memory space to store the many Multicast trees.

A participant who has left the Multicast data stream can return to the Multicast data stream again. This procedure is known as Grafting. Grafting enables the participant to receive Multicast data streams again before the hold time has elapsed.

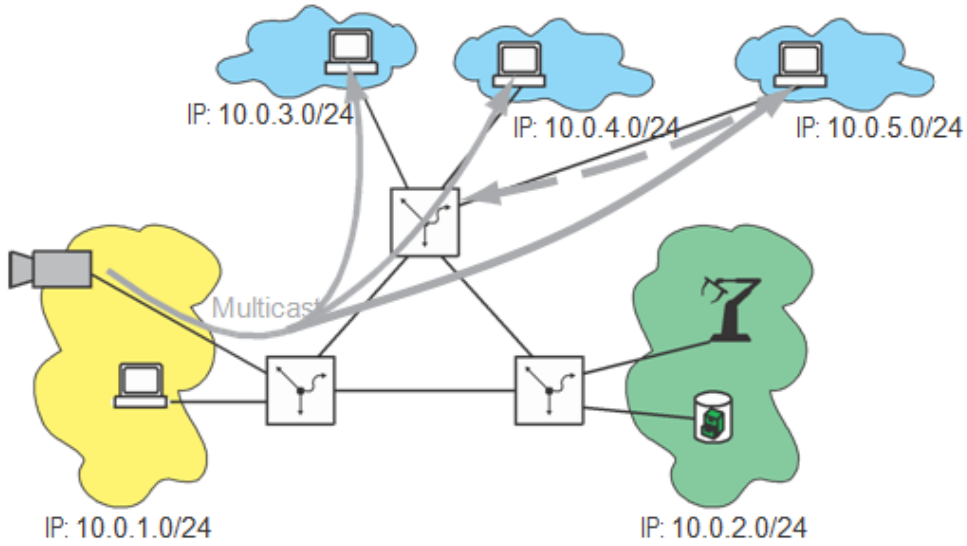


FIGURE 243 – Multicast Grafting

How PIM-SM functions

PIM-SM differs from PIM-DM and DVMRP with regard to the topology of the Multicast distribution:

- PIM-DM and DVMRP always use the direct paths (SPT - Shortest Path Tree) between the Multicast source and the Multicast recipients.
- With the standard setting, PIM-SM uses the path via a central transmission point (Rendezvous Point – RP). This path is known as the Rendezvous Point Tree (RPT). At the rendezvous point, the Multicast recipients report their interest in a Multicast group. The Multicast sources register at a rendezvous point and send the data exclusively to this rendezvous point, which forwards the data to the Multicast recipients. There is exactly one rendezvous point for each group. A PIM-SM router serves as the rendezvous point for one or more Multicast groups. The rendezvous point tree extends between the rendezvous point of the Multicast group and the Multicast recipients. The recipients of a Multicast group share this RPT as a shared tree. With this procedure, PIM-SM reduces the amount of stored tree information in the routes and thus reduces the processor load for the devices.

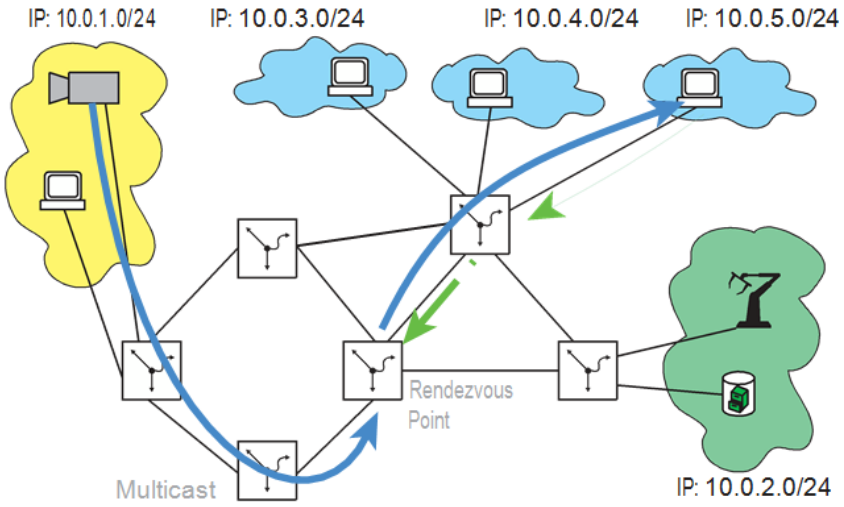


FIGURE 244 – Rendezvous Point in the PIM-SM protocol.

Depending on the application, there are shorter paths between the Multicast recipients and the Multicast source than the rendezvous point tree. In these cases, PIM-SM enables a switch to the direct path SPT. If the data rate for the Multicast transmission via the RPT exceeds a configurable threshold value, the router of the Multicast recipient unsubscribes from the rendezvous point. Instead, the router of the Multicast recipient creates a direct link to the last router before the Multicast source.

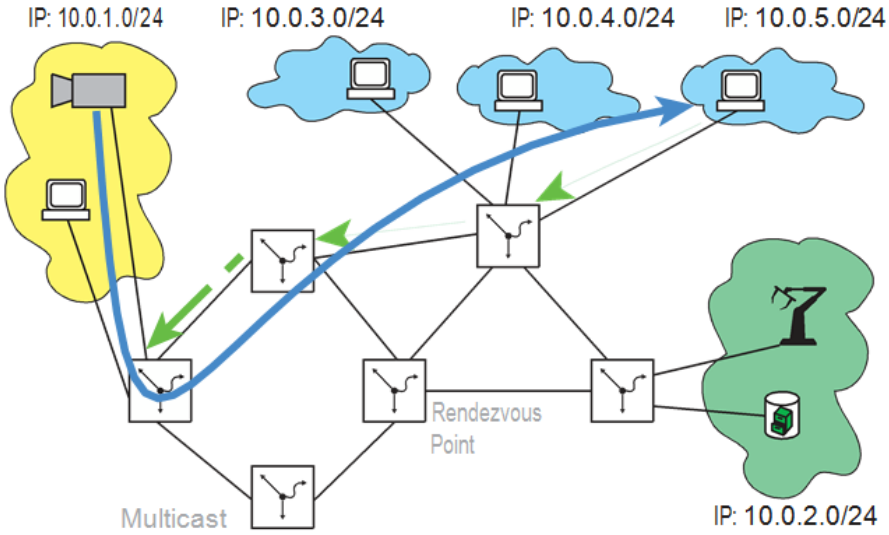


FIGURE 245 – Topology change from the RPT to the direct path (STP)

Designated Router

A participant who is interested in a Multicast group sends a corresponding IGMP message to the next reachable router. This router then sends a join message in the direction of the rendezvous point. If there are additional routers between the sending router and the rendezvous point, these forward the join message. This transmission ends either at the rendezvous point itself or at an already existing branch of the RPT. After the participant subscribes, PIM-SM creates or extends the path between the rendezvous point and the participant. When a participant unsubscribes from a Multicast group, the next router reachable from the participant sends a prune message to the rendezvous point. The prune message thus removes the related branch from the RPT.

In a network with multiple PIM-SM routers, exactly one router takes over the transmission of the join and prune messages between the Multicast recipients and the rendezvous point. In the following figure, this procedure is represented by green arrows. On the side of the Multicast sources, one of the PIM-SM routers also registers the available Multicast groups at the rendezvous point. The figure uses blue arrows to show this procedure.

These routers are called designated routers (DR). In the standard setting, the routers select the designated router using the IP address. The PIM-SM router with the highest IP address in a network segment takes over the task of the designated router. The DR selection can be controlled by setting a special priority for the designated routers. In this case, the router with the highest priority takes over the tasks of the designated router. The IP address is only used in the selection process if the priorities are the same.

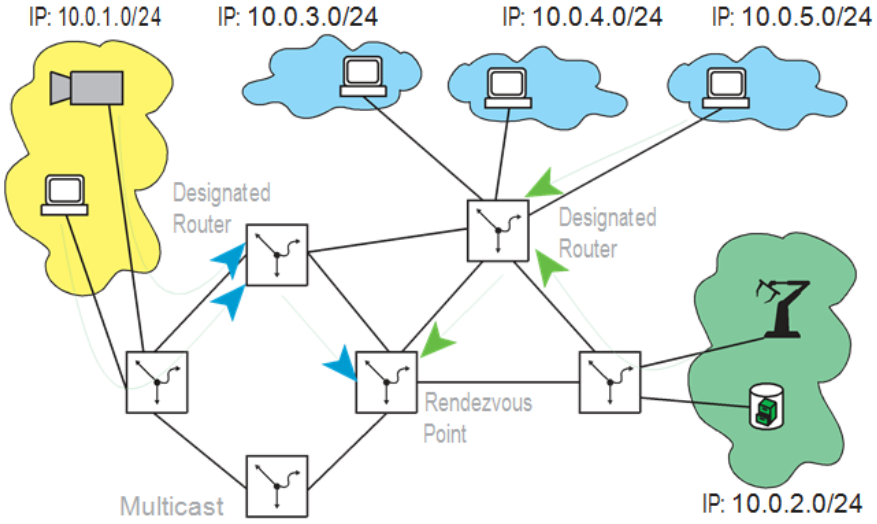


FIGURE 246 – Designated routers forward messages from Multicast sources and Multicast participants to the rendezvous point

Bootstrap router

PIM-SM provides two procedures for selecting the rendezvous point for a Multicast group:

- **Static RP configuration**

  In this procedure, one of the routers in the network is fixed as the rendezvous point for a Multicast group. The other routers contain the IP address of this router and the address of the related Multicast group in their configuration.

- **Dynamic RP configuration based on the Bootstrap Router procedure (BSR)**

  In this procedure, the routers in the network determine the rendezvous point dynamically. A router has the option to offer itself as a candidate for the task of rendezvous point. The dynamic procedure uses bootstrap messages to select the rendezvous point for a Multicast group. The bootstrap messages also inform the other routers in the PIM-SM domain about the router selected as the rendezvous point. The PIM-SM routers forward the Bootstrap messages within the PIM- SM domain. The PIM-SM domain consists of all the reachable routers with an activated PIM-SM protocol. An active PIM-SM router has

the option of limiting the domain as a BSR border. A router configured in this way drops the received BSR messages.

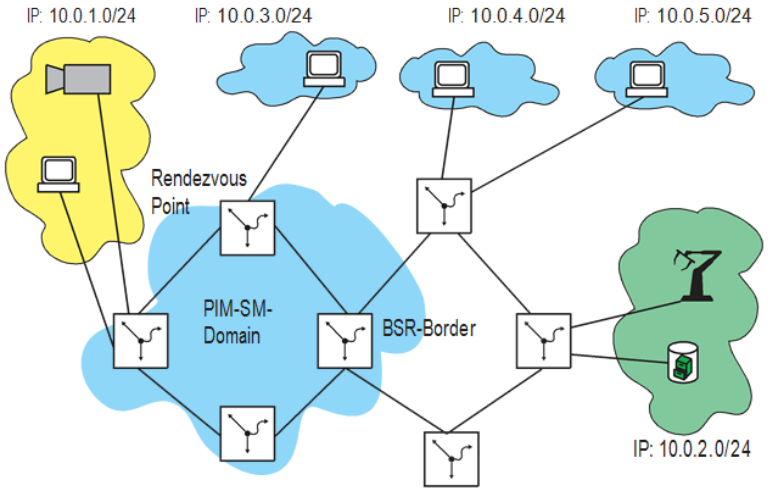


FIGURE 247 – Routers in the configuration as BSR borders drop bootstrap messages and limit the PIM-SM domain.

Scoping

In the Multicast transmission, the protocol provides two options for limiting the expansion of the Multicast data stream:

- Multicast Address Scoping / Boundary
  In the Multicast Address Scoping, the administrator assigns a Multicast IP address range to a router interface (see table 14). The router interface blocks the Multicast data streams with addresses within this address range.
  Example: `ip mcast boundary 239.193.122.0 255.255.255.0`
  In this example, the router interface blocks Multicast data streams with a Multicast IP address in the range 239.193.122.0-239.193.122.255.
- TTL Scoping
  Every Multicast data packet contains a TTL (Time To Live). The TTL is a counter which each router de-increments when it transmits a Multicast data packet. In TTL Scoping, the administrator assigns a TTL threshold to an interface. The router interface blocks every Multicast data packet for which the TTL is below the TTL threshold.
  Example: `ip multicast ttl threshold 64`
  In this example, the router interface blocks Multicast data streams with a TTL whose value is less than 64.

TTL	Scope
0	Restricted to the same host
1	Restricted to the same subnet
< 32	Restricted to a particular location, organization or department
< 64	Restricted to the same region
< 128	Restricted to the same continent
< 255	Unrestricted, global

Table 55: Usual scope for TTLs

Multicast Configuration

Select the Multicast protocol that best suits the application. As the Multicast routing protocols use different methods for the Multicast transmission, the router prevents the user from using more than one Multicast routing protocol at the same time. When one Multicast routing protocol is activated, the router deactivates any other active Multicast routing protocol.

Example with Layer 3 Redundancy

The Multicast configuration consists of the following steps:

- Configure the routing function on the participating routers for example, with OSPF
- Specify Multicast addresses, if applicable.
- Configure router interfaces. This also includes
  - specifying the Multicast boundaries,
  - activating IGMP
  - activating the selected Multicast routing protocol.
- Globally activate IGMP and therefore also IGMP Snooping.
- Globally activate the Multicast routing protocol.
- Activate Multicast transmission (forwarding).

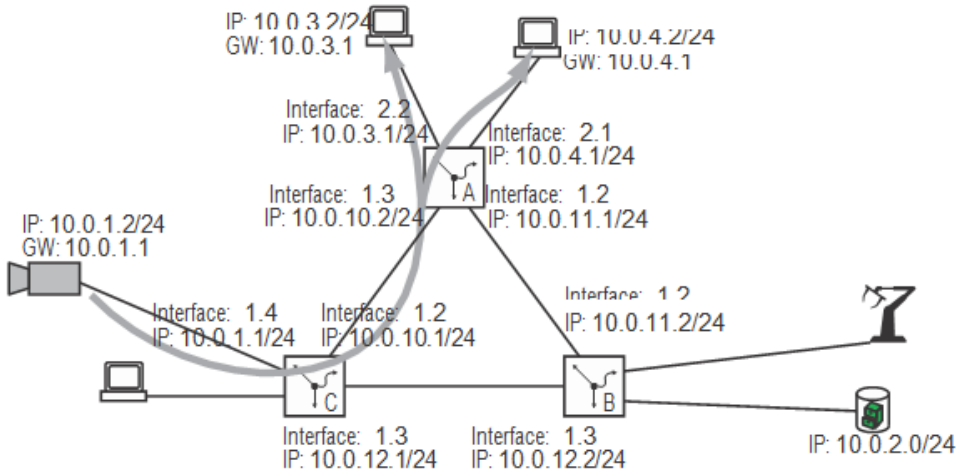


FIGURE 248 – Multicast example configuration

Configure router interfaces using the example of router A.

`enable`	**Switch to the Privileged EXEC mode.**
`configure`	**Switch to Configure mode.**
`interface 2/1`	**Configure the first interface.**
`ip multicast ttl-threshold 3`	**Set the TTL threshold for Multicast packets. See section on scoping for additional information.**
`ip igmp`	**Enable igmp on the port.**
`ip pimdm mode`	**Enable PIM-DM on the interface.**
`exit`	**Exit interface configuration.**
`interface 2/2`	**Configure the first interface.**

`ip multicast ttl-threshold 3`	**Set the TTL threshold for Multicast packets. See section on scoping for additional information.**
`ip igmp`	**Enable igmp on the port.**
`ip pimdm mode`	**Enable PIM-DM on the interface.**
`exit`	**Exit interface configuration.**
`interface 1/3`	**Configure the first interface.**
`ip multicast ttl-threshold 3`	**Set the TTL threshold for Multicast packets. See section on scoping for additional information.**
`ip igmp`	**Enable igmp on the port.**
`ip pimdm mode`	**Enable PIM-DM on the interface.**
`exit`	**Exit interface configuration.**

Next, globally activate IGMP for Router A.

`ip igmp`	**Globally activate IGMP on the switch.**

Next globally activate Multicast for Router A.

`ip pimdm`	**Enable the PIM-DM protocol globally.**
`ip multicast`	**Activate Multicast forwarding.**
`exit`	**Exit the config mode.**

FIGURE 249 – Multicast configuration using CLI.

Next check the Multicast routing settings.

`show ip pimdm` **Query the PIM-DM settings.**

```
Admin Mode..................................... Enable
Holdtimes...................................... 210 seconds

    PIM-DM INTERFACE STATUS
Interface Interface Mode  Protocol State
--------- --------------- ---------------
1/3       Enable          Operational
2/1       Enable          Operational
2/2       Enable          Operational
```

`show ip mcast` **Display the Multicast settings.**

```
Admin Mode..................................... Enable
Protocol State................................. Operational
Table Max Size ................................ 512
Number of Packets For Which Source Not Found .. 0
Number of Packets For Which Group Not Found ... 0
Protocol....................................... PIMDM
Entry Count ................................... 0
Highest Entry Count ........................... 0
```

`show ip mcast mroute summary` **Display the Multicast Multiroute summary.**

```
                 Multicast Route Table Summary
                                          Incoming  Outgoing
Source IP       Group IP        Protocol Interface Interface List
--------------- --------------- -------- --------- ---------------
10.0.1.159      239.192.1.1     PIMDM    1/3        2/1
```

```
10.0.1.159      239.192.1.1     PIMDM    1/3        2/2
show ip igmp                    Display the IGMP status.
IGMP Admin Mode.............................. Enable
DSCP value for frames routed in software..... 48(cs6)

    IGMP INTERFACE STATUS
Interface Interface Mode  Protocol State
--------- --------------- --------------
1/2       Enable          Operational
1/3       Enable          Operational
2/1       Enable          Operational
2/2       Enable          Operational
show ip igmp interface 1/3  Display the IGMP settings for the interface.
Slot/Port.................................... 1/3
IGMP Admin Mode.............................. Enable
Interface Mode............................... Enable
IGMP Version................................. 2
Query Interval (secs)........................ 125
Query Max Response Time (1/10 of a second)..... 100
Robustness................................... 2
Startup Query Interval (secs) ............... 1
Startup Query Count.......................... 2
Last Member Query Interval (1/10 of a second).. 10
Last Member Query Count...................... 2
```

FIGURE 250 – Validating Multicast configuration using CLI.

Configure the Magnum 12KX switch B and Magnum 12KX switch C in the same way as Magnum 12KX switch A.

Example with Layer 2 Redundancy (Ring Structure)

VLAN 1 is assigned to the Ring topologies so information can be exchanged at Layer 2.

Assign other VLAN IDs to the connected VLANs and leave the Ring on its own in VLAN 1. We thus enable the transmission of the Multicast data streams on Layer 3.

If multiple VLANs are assigned to the Ring as transfer networks, then the Switch transmits the Multicast data streams to every transfer network during the flood and prune phases. This means that the Switch transmits the Multicast data streams to every VLAN and the network load is thus multiplied in the Ring.

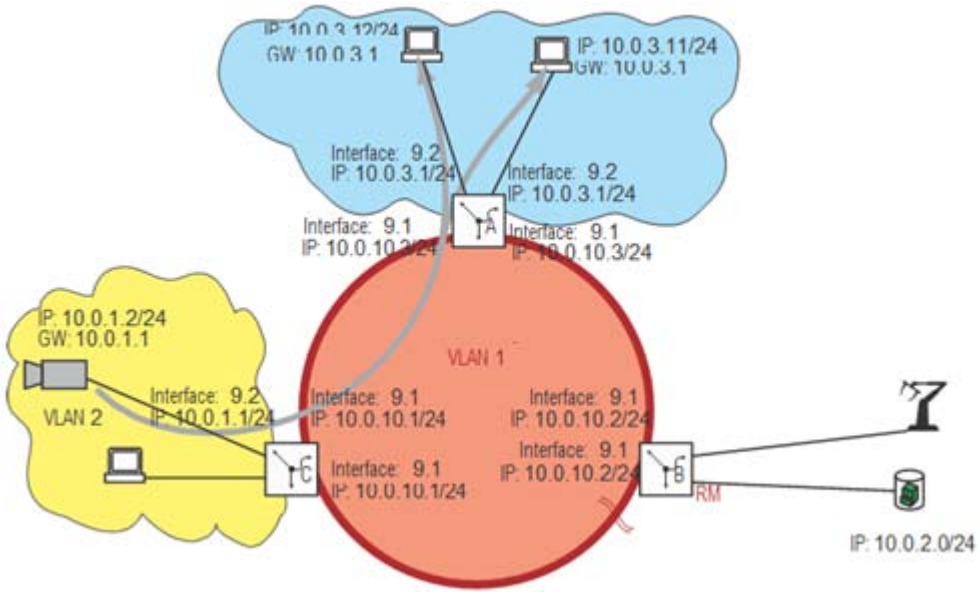


FIGURE 251 – Multicast example configuration for a Ring.

Tips for the configuration

Selection of the PIM-DM Multicast routing protocol
Select PIM-DM if the application requires fast switching times and is able to tolerate any packet duplications during the switching time. Set fast switching times by reducing the “Hello Time”. Packet duplications occur when multiple routers are connected to a subnetwork. In this case, the Assert Process clarifies which router is permitted to send into the subnetwork. Until this is clarified, all routers send into this subnetwork.

Selection of the DVMRP Multicast routing protocol
Select DVMRP if the application does not tolerate packet duplications and is content with higher switching times. DVMRP provides a big advantage when using subdivided subnetwork/VLANs in a Ring. Using its own Multicast routing tables, DVMRP already knows the topology and thus prevents packet duplications.

Selection of the PIM-SM Multicast routing protocol
Select PIM-SM if the application has few participants and the user can tolerate longer paths for the application. In this case, PIM-SM has the advantage that the data volume created in the routers remains small.

Configuration as Rendezvous Point for PIM-SM
When using PIM-SM, The user has the option of defining a router as a rendezvous point candidate for a Multicast group. To do this, specify the Multicast group for which the router can be used as the rendezvous point.

`enable`	**Switch to the Privileged EXEC mode.**
`configure`	**Switch to Configure mode.**
`ip pimsm rp-candidate 2/1 224.0.0.0/24`	**Activate the router as the potential rendezvous point for group 244.0.0.0/24.**
`no ip pimsm rp-candidate 2/1`	**Deactivate the router as a potential rendezvous point.**

FIGURE 252 – Configuring Rendezvous point for PIM-SM

Configuration of the limit for the switch to SPT

When using PIM-SM, The user has the option of defining the limit for the switch to SPT on the last routers for the Multicast recipients. To do this, specify the limit for the data throughput in Kbit/s, and when this limit is reached the router switches to the shortest path SPT.

`enable`	**Switch to the Privileged EXEC mode.**
`configure`	**Switch to Configure mode.**
`ip pimsm spt-threshold 1000`	**Activate the limit of 1000 Kbit/s for the switch to the SPT.**
`no ip pimsm spt-threshold`	**Deactivate the limit for the switch to the SPT.**

FIGURE 253 – Configuring rendezvous point for PIM-SM.

Configuration as Designated Router for PIM-SM

When using PIM-SM, The user has the option of defining a router as the designated router candidate. To do this, specify the priority with which the router offers itself as the designated router.

`enable`	**Switch to the Privileged EXEC mode.**
`configure`	**Switch to Configure mode.**
`ip pimsm dr-priority 2/1 priority 2000`	**Activate the router as the potential designated router with the priority 2000.**
`no ip pimsm dr-priority 2/1`	**Deactivate the router as a potential designated router.**

FIGURE 254 – Configuring Designated Router for PIM-SM.

Configuration as Bootstrap Router for PIM-SM

When using PIM-SM, The user has the option of defining a router as the bootstrap router candidate. To do this, specify the priority with which the router offers itself as the bootstrap router.

`enable`	**Switch to the Privileged EXEC mode.**
`configure`	**Switch to Configure mode.**
`ip pimsm bsr-candidate 2/1 priority 20`	**Activate the router as the potential bootstrap router with the priority 20.**
`no ip pimsm bsr-candidate 2/1`	**Deactivate the router as a potential bootstrap router.**

FIGURE 255 – Configuring Bootstrap Router for PIM-SM.

Limiting the PIM-SM domain

When an interface of the device is defined as a BSR border, the router does not forward any BSR messages via this interface. In this way, the router limits the PIM-SM domain.

`enable`	**Switch to the Privileged EXEC mode.**
`configure`	**Switch to Configure mode.**

`interface 2/1`	**Configure the interface.**
`ip pimsm bsr-border`	**Deactivate the forwarding of BSR messages via interface.**
`no ip pimsm bsr-border`	**Allow the forwarding of BSR messages via interface.**

FIGURE 256 – Limiting the PIM-SM Domain.

Reducing the switching times

With both DVMRP and PIM-DM the user can reduce the switching times by reducing the IGMP Querier Interval on the router interface. This reduction becomes effective when an inactive router to which Multicast recipients are connected becomes active again.

`enable`	**Switch to the Privileged EXEC mode.**
`configure`	**Switch to Configure mode.**
`interface 2/1`	**Configure the interface.**
`ip igmp query-max-response-time 1`	**Set the Query Max Response Time smaller than the query interval. In this example 1 second. Default is 10 seconds.**
`ip igmp query-interval 5`	**Set the query interval to 5 seconds. Default is 125 seconds.**
`ip pimdm query-interval 1`	**Set the PIM-DM query interval (Hello Time) to 1 second. Default setting is 30 seconds. With PIM-DM, when the Hello Time is reduced, a router can detect more quickly when a downstream router changes state.**

FIGURE 257 – Multicast settings with reduced querier time.

With PIM-DM, using a default route that has been entered can reduce the switching time. While the router is gathering information about the path to the source (RPF), the router can use a default route that has been entered.

Special feature of VLAN routing

The router floods a Multicast data stream to all ports of a VLAN routing interface if

- The Multicast data stream comes from another subnetwork and
- At least one recipient on this VLAN interface has registered via IGMP for this Multicast data stream.

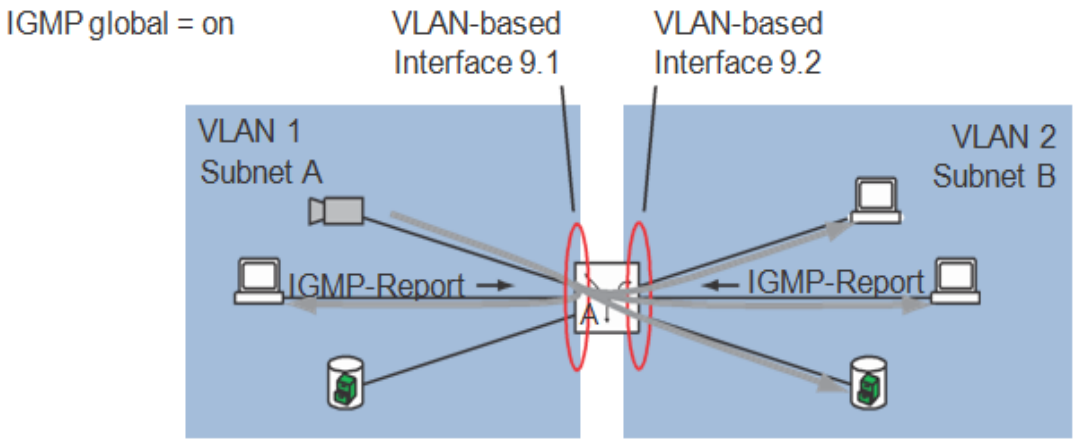


FIGURE 258 – Registered Multicast data stream on the VLAN routing interface

APPENDIX 1

Other relevant information

Management Information Base (MIB)

The Management Information Base (MIB) is designed in the form of an abstract tree structure.
The branching points are the object classes. The "leaves" of the MIB are called generic object classes.
If this is required for unique identification, the generic object classes are instantiated, i.e. the abstract structure is mapped onto reality, by specifying the port or the source address.
Values (integers, time ticks, counters or octet strings) are assigned to these instances; these values can be read and, in some cases, modified. The object description or object ID (OID) identifies the object class. The subidentifier (SID) is used to instantiate them.

Example:
The generic object class
`hmPSState (OID = 1.3.6.1.4.1.248.14.1.2.1.3)`
is the description of the abstract information "power supply status". However, it is not possible to read any information from this, as the system does not know which power supply is meant.
Specifying the subidentifier (2) maps this abstract information onto reality (instantiates it), thus indicating the operating status of power supply 2. A value is assigned to this instance and can then be read. The instance "get `1.3.6.1.4.1.248.14.1.2.1.3.2`" returns the response "1", which means that the power supply is ready for operation.

The following abbreviations are used in the MIB:	
Comm	Group access rights
con	Configuration
Descr	Description
Fan	Fan
ID	Identifier
Lwr	Lower (e.g. threshold value)
PS	Power supply
Pwr	Power supply
sys	System
UI	User interface
Upr	Upper (e.g. threshold value)
ven	Vendor = manufacturer (Hirschmann)

Definition of the syntax terms used:	
Integer	An integer in the range -2^{31} - 2^{31}-1
IP Address	xxx.xxx.xxx.xxx (xxx = integer in the range 0-255)
MAC Address	12-digit hexadecimal number in accordance with ISO/IEC 8802-3
Object identifier	x.x.x.x… (e.g. 1.3.6.1.1.4.1.248…)

Octet string	ASCII character string
PSID	Power supply identifier (number of the power supply unit)
TimeTicks	Stopwatch, Elapsed time (in seconds) = numerical value / 100 Numerical value = integer in range $0\text{-}2^{32}\text{-}1$
Timeout	Time value in hundredths of a second Time value = integer in range $0\text{-}2^{32}\text{-}1$
Type field	4-digit hexadecimal number in accordance with ISO/IEC 8802-3
Counter	Integer ($0\text{-}2^{32\text{-}1}$), whose value is increased by 1 when certain events occur.

The MIBs can be downloaded from the GarrettCom web site.

APPENDIX 2

List of RFCs

RFC-768	UDP
RFC-778	Internet Clock Service
RFC-783	TFTP
RFC-791	IP
RFC-792	ICMP
RFC-793	TCP
RFC-826	ARP
RFC-854	Telnet
RFC-855	Telnet Option
RFC-891	Local Network Protocols
RFC-894	Transmission of IP Datagrams over Ethernet Networks
RFC-896	Congestion Control in IP/TCP Networks
RFC-919	IP Broadcast
RFC-922	IP Broadcast in the presence of subnets
RFC-950	IP Subnetting
RFC-951	BOOTP
RFC-1027	Using ARP to implement Transparent Subnet Gateways Proxy ARP
RFC-1058	RIP
RFC-1112	Host Extensions for IP Multicasting
RFC-1155	SMIv1
RFC-1157	SNMPv1
RFC-1212	Concise MIB Definitions
RFC-1213	MIB2 NSSA Option
RFC-1256	ICMP Router Discovery Messages
RFC-1321	Message Digest Algorithm
RFC-1340	Assigned Numbers
RFC-1493	Dot1d
RFC-1519	CIDR
RFC-1542	BOOTP-Extensions
RFC-1587	NSSA (OSPF)

RFC-1643	Ethernet-like-MIB
RFC-1724	RIP v2 MIB Extension
RFC-1757	RMON
RFC-1765	OSPF Database Overflow
RFC-1769	SNTP
RFC-1812	Requirements for IP Version 4 Routers
RFC-1850	OSPF MIB
RFC-1867	HTML/2.0 Forms w/ file upload extensions
RFC-1901	Community based SNMP v2
RFC-1905	Protocol Operations for SNMP v2
RFC-1906	Transport Mappings for SNMP v2
RFC-1907	Management Information Base for SNMP v2
RFC-1908	Coexistence between SNMP v1 and SNMP v2
RFC-1945	HTTP/1.0
RFC-2030	SNTP v4
RFC-2068	HTTP/1.1 protocol as updated by Draft-ietf-http-v11-spec-rev-03
RFC-2082	RIP-2 MD5 Authentication
RFC-2131	DHCP
RFC-2132	DHCP-Options
RFC-2233	The Interfaces Group MIB using SMI v2
RFC-2236	IGMPv2
RFC-2246	The TLS Protocol, Version 1.0
RFC-2271	SNMP Framework MIB
RFC-2328	OSPF
RFC-2328	OSPF Version 2
RFC-2338	VRRP
RFC-2346	AES Cipher suites for Transport Layer Security
RFC-2362	PIM-SM
RFC-2365	Administratively Scoped Boundaries
RFC-2453	RIP v2
RFC-2570	Introduction to SNMP v3
RFC-2571	Architecture for Describing SNMP Management Frameworks
RFC-2572	Message Processing and Dispatching for SNMP
RFC-2573	SNMP v3 Applications
RFC-2574	User Based Security Model for SNMP v3
RFC-2575	View Based Access Control Model for SNMP
RFC-2576	Coexistence between SNMP v1,v2 & v3

RFC-2578	SMI v2
RFC-2579	Textual Conventions for SMI v2
RFC-2580	Conformance statements for SMI v2
RFC-2597	Assured Forwarding
RFC-2598	An Expedited Forwarding PHB
RFC-2613	SMON
RFC-2618	RADIUS Authentication Client MIB
RFC-2620	RADIUS Accounting MIB
RFC-2674	Dot1p/Q
RFC-2787	VRRP MIB
RFC-2818	HTTP over TLS
RFC-2851	Internet Addresses MIB
RFC-2863	The Interfaces Group MIB
RFC-2865	RADIUS Client
RFC-2866	RADIUS Accounting
RFC-2868	RADIUS Attributes for Tunnel Protocol Support
RFC-2869	RADIUS support for EAP
RFC-2932	IPv4 Multicast Routing MIB
RFC-2933	IGMP MIB
RFC-2934	PIM MIB for IPv4
RFC-3046	DHCP/BootP Relay
RFC-3101	The OSPF Not So Stubby Area
RFC-3164	The BSD Syslog Protocol
RFC-3376	IGMPv3
RFC-3580	802.1X RADIUS Usage Guidelines
RFC-3768	VRRP, Virtual Router Redundancy Protocol
RFC-4330	SNTP, obsoletes # 1769 and 2330

Draft-holbrook-idmr-igmpv3-ssm-08.txt	IGMPv3 / MLDv2 for SSM
Draft-ietf-idmr-dvmrp-mib-11.txt	DVMRP MIB
Draft-ietf-idmr-dvmrp-v3-10	DVMRP
Draft-ietf-magma-igmpv3-and-routing-05.txt	IGMPv3 an Multicast Routing Protocol Interaction
Draft-ietf-magma-mgmd-mib-03.txt	Multicast Group Membership Discovery MIB
Draft-ietf-pim-v2-dm-03	PIM-DM
Draft-ietf-smm-arch-06.txt	Source -Specific Multicast for IP
Draft-ietf-ipv6-RFC2096-update-07.txt	IP Forwarding Table MIB

APPENDIX 3

List of IEEE Standards

IEEE 802.1AB Topology Discovery (LLDP)

IEEE 802.1D Switching, GARP, GMRP, Spanning Tree (Supported via 802.1S implementation)

IEEE 802.1D-1998 Media Access Control (MAC) Bridges (includes IEEE 802.1p Priority and Dynamic Multicast Filtering, GARP, GMRP)

IEEE 802.1P Traffic class expediting and dynamic multicast filtering incorporated into IEEE 802.1D and IEEE-802.1AC

IEEE 802.1Q-1998 Virtual Bridged Local Area Networks (VLAN Tagging, Port Based VLANs, GVRP)

IEEE 802.1S Multiple Spanning Tree

IEEE 802.1V Protocol Based VLANs

IEEE 802.1W.2001 Rapid Reconfiguration, Supported via 802.1S implementation

IEEE 802.1X Port Authentication

IEEE 802.3 2002 Ethernet

IEEE 802.3AC VLAN Tagging

IEEE 802.3AF PoE Standard

IEEE 802.3AD Link Aggregation with Static LAG and LACP support

IEEE 802.3X Flow Control

IEEE 1588 Standard for A Precision Clock Synchronization Protocol for Networked Measurement and Control Systems

IEEE 1588-2008 Same as IEEE 1588 modified to support PTP-v2

APPENDIX 4

Abbreviations Used

ABR	Area Border Router
ACA	Auto Configuration Adapter
ACL	Access Control List
AS	Autonomous System
ASBR	Autonomous System Border Router
BC	Broadcast
BDR	Backup designated Router
BGP	Border Gateway Protocol
BOOTP	Bootstrap Protocol
CIDR	Classless Inter Domain Routing
CLI	Command Line Interface
DHCP	Dynamic Host Configuration Protocol)
DR	Designated Router
DVMRP	Distance Vector Multicast Routing Protocol
EUI	Extended Unique Identifier
F/O	Fiber Optic
FDB	Forwarding Database
GARP	General Attribute Registration Protocol
GMRP	GARP Multicast Registration Protocol
HTTP	Hypertext Transfer Protocol
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
IGMP	Internet Group Management Protocol
IGP	Interior Gateway Protocol
IP	Internet Protocol
LED	Light Emitting Diode
LLDP	Link Layer Discovery Protocol
LSA	Link Status Advertisement
LSD	Link State Database

MAC	Media Access Control
MC	Multicast
MSTP	Multiple Spanning Tree Protocol
NSSA	Not So Stubby Area
NTP	Network Time Protocol
OSPF	Open Shortest Path First
OUI	Organizationally Unique Identifier
PC	Personal Computer
PIM-DM	Protocol Independent Multicast-Dense Mode
PIM-SM	Protocol Independent Multicast-Sparse Mode
PTP	Precision Time Protocol
QoS	Quality of Service
RFC	Request For Comment
RIP	Routing Information Protocol
RM	Redundancy Manager
RPF	Reverse Path Forwarding
RS	Rail Switch
RSTP	Rapid Spanning Tree Protocol
SFP	Small Form-factor Pluggable
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SPT	Shortest Path Tree
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TP	Twisted Pair
TTL	Time-to-live
UDP	User Datagram Protocol
URL	Uniform Resource Locator
UTC	Coordinated Universal Time
VL	Virtual Link
VLAN	Virtual Local Area Network
VLSM	Variable Length Subnet Mask
VRID	Virtual Router Identification
VRRP	Virtual Router Redundancy Protocol

Index